BlipNet Administrators Guide

Table Of Contents

Getting Started 1
Introduction to BlipManager 4
General information about views 6
  BlipManager Views 6
Configuration View 9
BlipNode View 10
Terminal View 11
General 12
Allowed Terminals 14
Power Control 15
Wireless Control 17
Advanced 18
Version Info 20
Server Info 22
BlipNode Configurations 24
BlipNode Groups 26
Advanced 27
User Accounts 30
Allowed BlipNodes 31
Security 32
Terminals 34
  Add 35
  Remove 37
  Edit 37
Mobility Settings 38
Mobility Zones 39
General 42
  BlipNet Mobility 42
  Security 42
General about BlipNode Configurations 44
  Client Node 44
  Tracking Node 44
  Server Node 45
  Unconfigured 48
Making a new BlipNode Configuration 49
Configuration Name 50
BlipNode Accessibility 51
BlipNode Services 54
BlipNode Services 56
  LAN Access Profile Settings 56
  WAP Over Bluetooth Settings 57
  Personal Area Network Profile Settings 59
  Personal Area Network Protocol Settings 60
  Object Push Server Settings 62
  File Transfer Server Settings 64
BlipNet Mobility Service 65
  Mobility Zones 65
  Supported Devices 65
  Pre-configuring BlipNodes 65
About Wireless BlipNodes 67
Using the BlipNode Groups Concept 69
Configuration of BlipNet for BlipNet API applications 70

Diagnostics..... 71
BlipNode does not connect to the BlipServer..... 72
Problem when connecting to LAN access service in BlipNet..... 74
Problem when connecting to the OPP server in BlipNet..... 75
Problem when pushing objects to the OPP server in BlipNet..... 76
Problem when pushing from BlipNet to an OPP server device..... 77
Terminology..... 78

Installing BlipNet

Getting Started

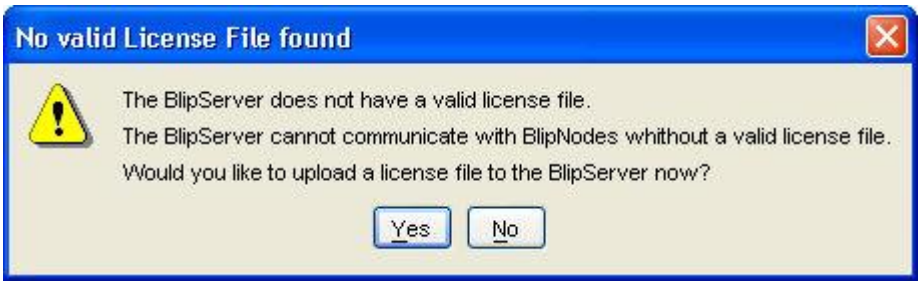
Follow these steps to get started:

1. Install BlipNet.
   Please refer to the **InstallationGuide.html** for a description of the installation process.

2. Start the BlipManager.
   a. Windows: Go to "Start->Programs->BlipNet->BlipManager".
   b. Linux: Go to "Main Menu->Programs->BlipNet->BlipManager" or from a x-terminal execute following file: /opt/blipnet/ blipmanager.bin (default location).

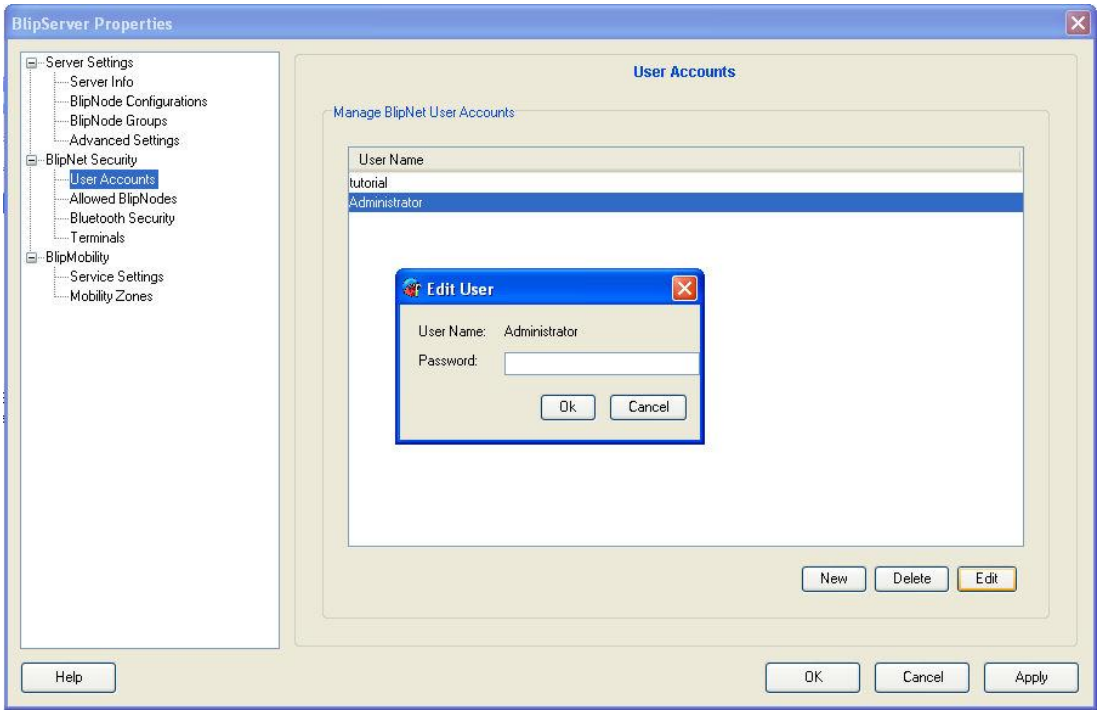
3. Login to the BlipManager.
   a. When running the BlipManager locally on the same machine as the BlipServer, only the password has to be supplied. The default password is "BLIPNET".
   b. When running the BlipManager on another machine than the BlipServer, the IP address of the machine with the BlipServer must be supplied the first time you login. Please see the Diagnostics section if you have problems connecting to the BlipServer remotely.

4. Uploading a License file.
   If your BlipNet installation does not contain valid License file, you will be prompted to upload one every time you start a BlipManager.
   The BlipServer will not be able to communicate with any BlipNodes, unless a valid license file is installed.

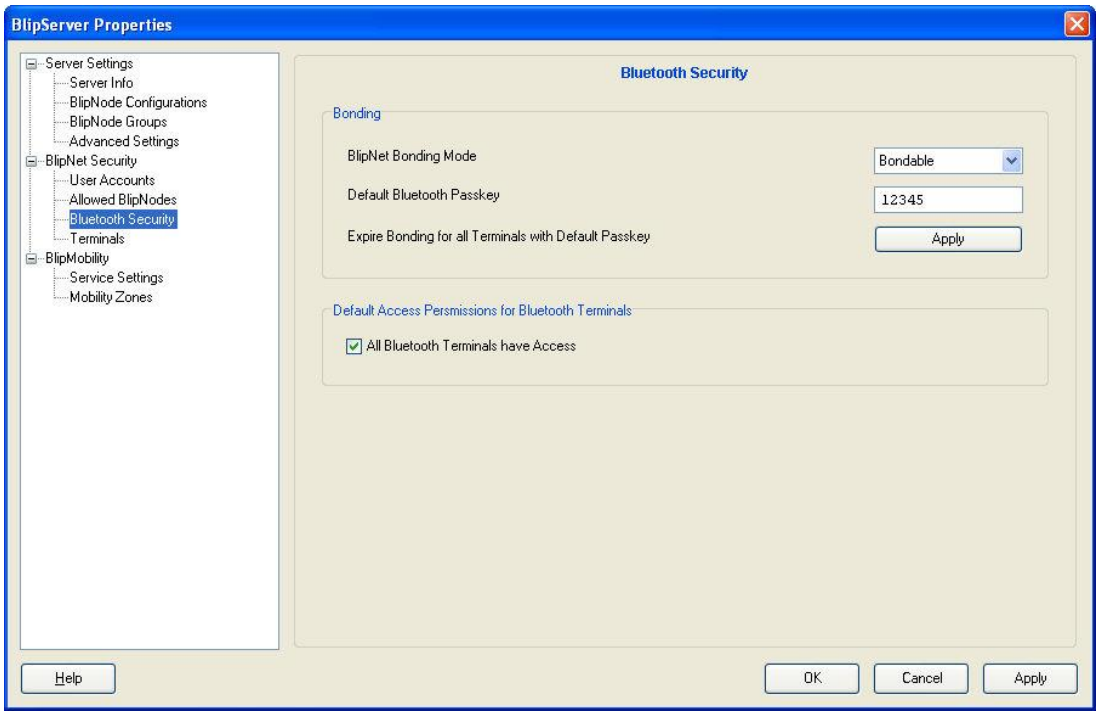

No valid License File found
The BlipServer does not have a valid license file.
The BlipServer cannot communicate with BlipNodes whithout a valid license file.
Would you like to upload a license file to the BlipServer now?
Yes
No

   Select Yes to upload the License file you have received from BLIP Systems.

5. Change Administrator password.
   When the BlipManager is started, it is recommended to change the administrator password. This is done by:
   a. In the menu bar select "File->Properties".
   b. In the BlipServer Properties window select the tab called "User Accounts".
   c. Select "Administrator" from the list and click on the "Edit" button and change the password. Make sure to remember this password.
   d. Click the "OK" button.



6. Specify a default Bluetooth Passkey.
   Assuming that the "Server Node (All Services)" configuration is selected, a default Bluetooth Passkey or dedicated Bluetooth Passkeys must be defined, please follow this procedure:
   a. In the menu bar select "File->Properties".
   b. In the BlipServer Properties window, select "Bluetooth Security".
   c. Specify a default passkey. All users who know this key will no have access to your system. If you want only specific devices to have access, de-select the "All Bluetooth Terminals have Access" option and follow the guide in the BlipServer - Terminals section to add your Bluetooth Terminals.



7. Connect the BlipNodes to the LAN and connect power.
   The BlipNodes will appear in the configuration view tree to the left in the BlipManager main window. Initially the BlipNodes will pop up in the "Unconfigured" configuration group folder.

8. Apply a configuration to a BlipNode.
   Assuming that the BlipNode shall be used for Bluetooth terminals to access the Internet, follow the steps:
   a. Right click on a BlipNode and select "Properties".
   b. The window "BlipNode Properties" will appear. In the "General" tab, find the list box called "Configuration" and select "Server Node (All Services)".
   c. It's also recommended to change the friendly name of the BlipNode.

The system is now in operation.

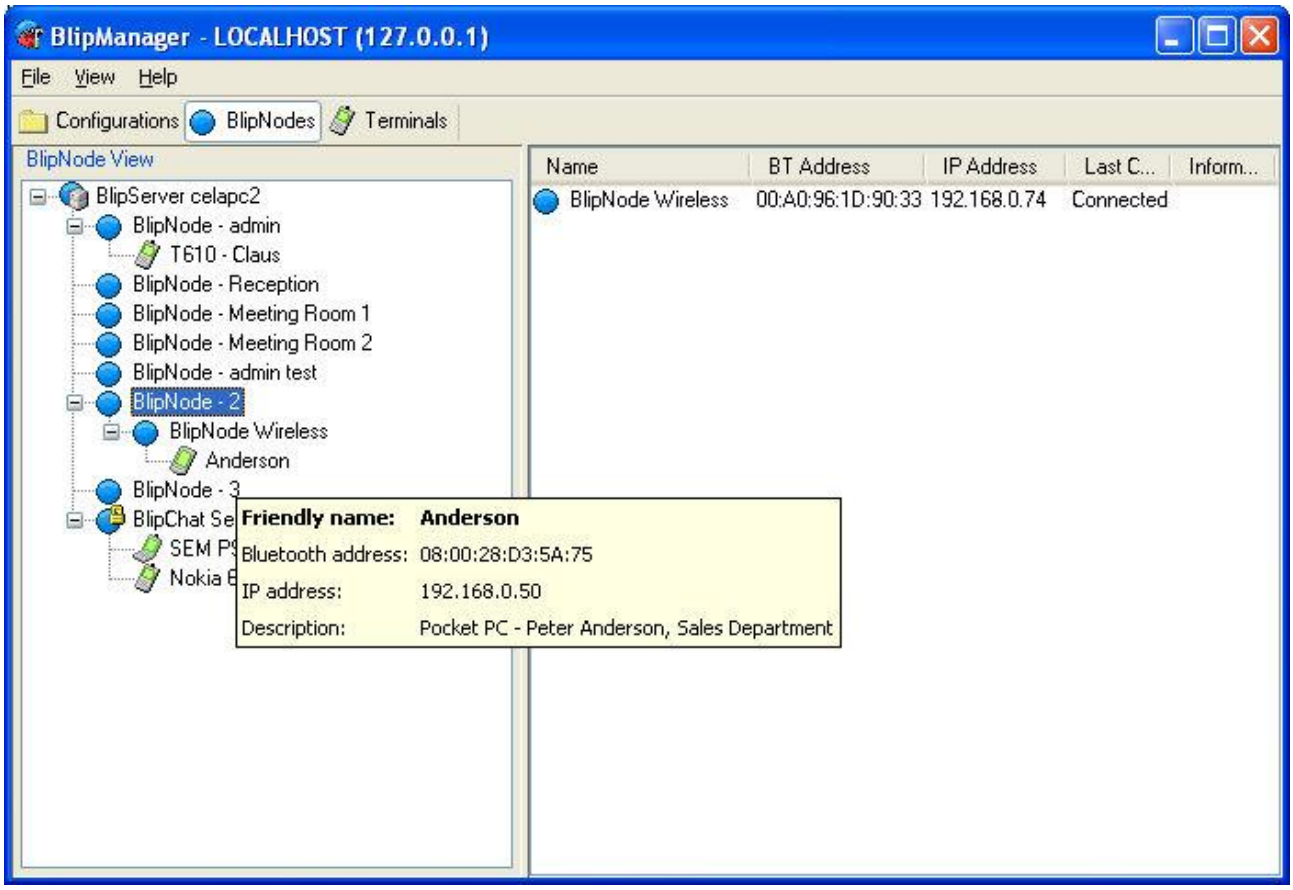
Important: Maintenance releases and releases with new features will be released from BLIP Systems. Please verify that your installation is up to date, by checking for new software on http://www.blipsystems.com. Section BlipServer - Advanced contains a description of how to upgrade the BlipNodes.

Introduction to BlipManager

The BlipNet system can be administered from the BlipNet management tool called BlipManager. The BlipManager can be used to:

- Administrate:
  - User Accounts
  - Allowed BlipNodes
  - Allowed Terminals
  - Security (Bluetooth Passkeys)
  - Software Updates
- Configure:
  - BlipNode Accessibility
  - Services in the BlipNodes
  - BlipNet Mobility
  - Wireless BlipNodes
- Monitor:
  - Status of the system
  - Connected terminals
  - Active sessions
  - BlipNode SW versions

The BlipManager is implemented as a thin client. It does not have any local storage. All configuration changes are made directly to the BlipServer. The BlipManager is supported on both Windows platform and Linux platforms. It is not necessary to run the BlipManager and the BlipServer on the same machine.



The figure above illustrates the BlipManager main window, which is split in two sub-windows. A sub-window showing a configuration view which includes a tree of BlipNet components and a sub-window showing detailed information of the items in the tree.

The Tree is updated automatically. This means that for example when a new terminal is connected it will be shown in the Configuration View tree automatically and removed automatically when it is disconnected.
If you want to refresh the tree manually, you can select refresh in the Menu or press the F5 key.

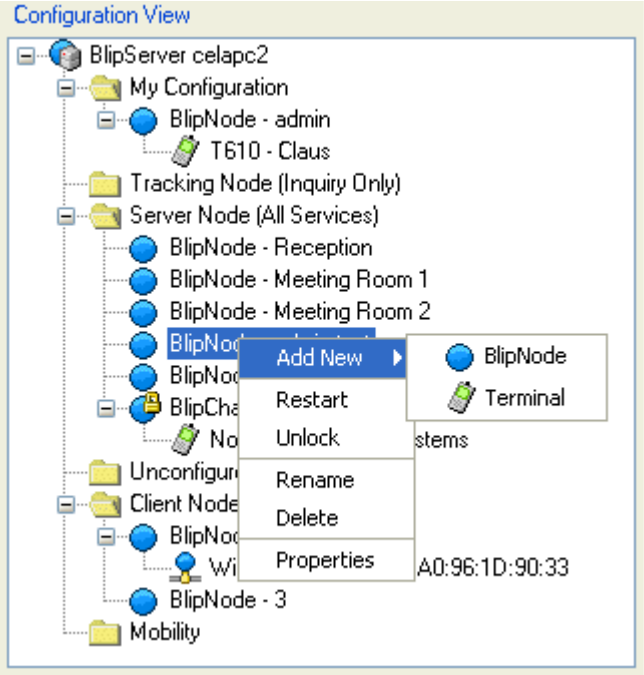
BlipManager Views

General information about views

BlipManager Views

The BlipManager has 3 different views that all shows the status of the BlipServer components in different ways.

In all views you can right click a component for a pop-up menu with different actions for the selected.



BlipServer

The BlipServer Icon represents the BlipServer that your BlipManager is currently connected to.

The Icon change to images to represent different conditions of the BlipServer:

The BlipServer is running
The connection to the BlipServer is lost. This means that either the BlipServer is not running or the network connection to the server is lost.

Right Click Actions

1. Add New
   Add new sub elements to the BlipServer. Includes BlipNodes, Configurations and Terminals.
2. Rename
   Change the Friendly name of the BlipServer

3. Properties
   Allow you to change the BlipServer properties. For more information read BlipServer Properties

Configuration

Only shown in configuration view.
Represents a configuration group that can contain a number of BlipNodes that are assigned to that configuration.

Right Click Actions

1. Add New BlipNode
   Add a new BlipNode to the BlipServer and assign it with the selected configuration.
2. Properties
   Brings up the Configuration Properties. For more information read Configuration Properties

BlipNode

The BlipNode represents a BlipNode that is attached to the BlipServer.

The Icon change to images to represent different conditions of the BlipNode.

The BlipNode is running and connected to the BlipServer
The BlipNode is running but might not be working correctly. Open the Properties for the BlipNode to read more about the warning.
The BlipNode is in use by a BlipNet Application.
Software upgrade is in progress. Do not perform any actions on this BlipNode until the Software upgrade has completed.
The BlipNode is not connected to the server. Reasons could be that the BlipNode is powered off, not allowed on the BlipServer or is not able to establish a TCP/IP Connection to the BlipServer.

Right Click Actions

1. Add New BlipNode
   Add a new BlipNode as a wireless BlipNode with the selected BlipNode as parent
2. Add New Terminal
   Allow you to search and add a new Bluetooth Terminal to BlipNet
3. Restart
   Restarts the BlipNode. All active Bluetooth connections will be lost.
4. Unlock
   If a BlipNode is in use by an application, the Administrator can override this by unlocking the BlipNode. The BlipNode will return to its original settings and will be available for other applications.
5. Rename
   Change the friendly name of the BlipNode. This is the Name Bluetooth Terminals will find when performing inquiry/name lookup.
6. Delete
   Disconnects and permanently delete all information and settings about the BlipNode, from the BlipServer.

7. Properties
   Brings up the Properties for the BlipNode. For more information read BlipNodeProperties

Terminal

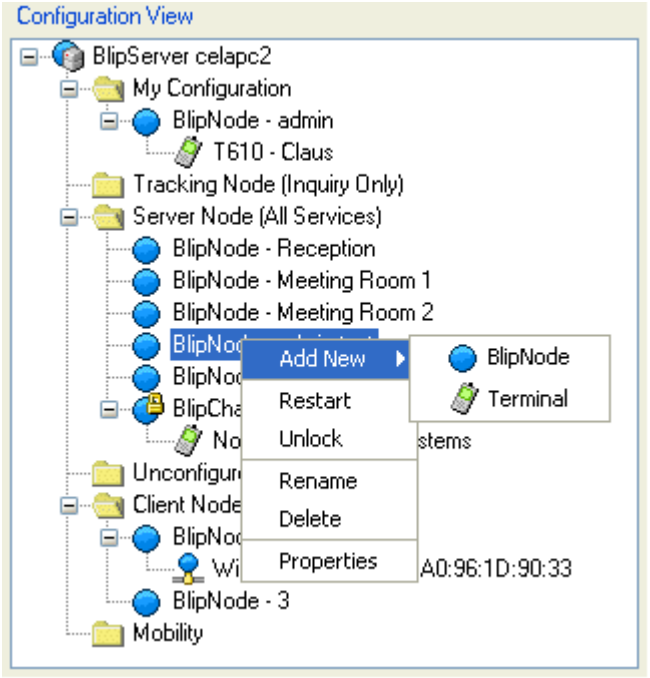
Represents a Bluetooth Terminal. The icon will represent the Class of Device type of the Bluetooth Terminal.

Right Click Actions

1. Disconnect
   Disconnects the Bluetooth Terminal from the BlipNode
2. Delete
   Only possible on not connected Terminals in Terminal view. Permanently delete all information about the terminal, including PIN key settings and description from the BlipServer.
3. Properties
   Brings up the Properties for the Terminals. For more information read TerminalProperties

Configuration View

Shows The BlipServer Configuration Groups with the BlipNodes belonging to each group.



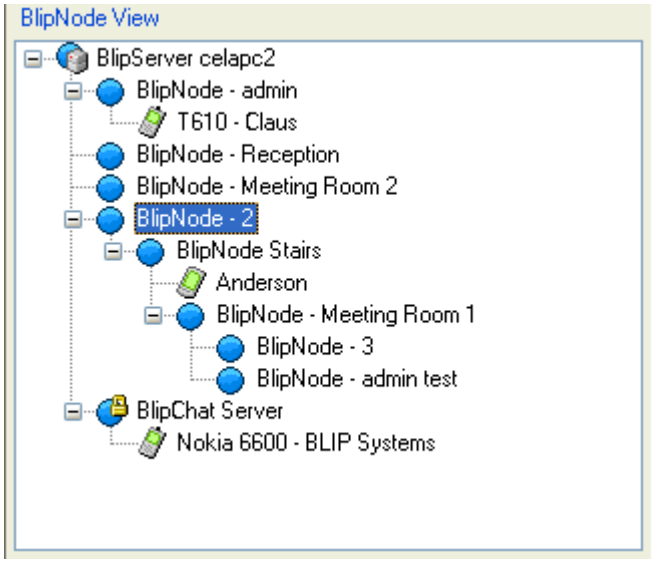
You can move BlipNodes between different configuration groups using Drag'n'Drop.

In the Menu you can choose to show empty configuration groups which will make the view display configurations groups even if no BlipNodes are attached to it.

Bluetooth Terminals will be show as children to BlipNodes when a Bluetooth connection exits between them.

BlipNode View

Shows the BlipNode structure. This is especially useful if you have wireless BlipNodes as the Tree will illustrate the Wireless Topology.



All BlipNodes shown as direct children to the BlipServer are BlipNodes connected to the Server through Ethernet.

A BlipNode show as a child to another BlipNode is a wireless BlipNode meaning that the wireless BlipNode is connected to the BlipServer with a Bluetooth PAN connection through the parent BlipNode(s).

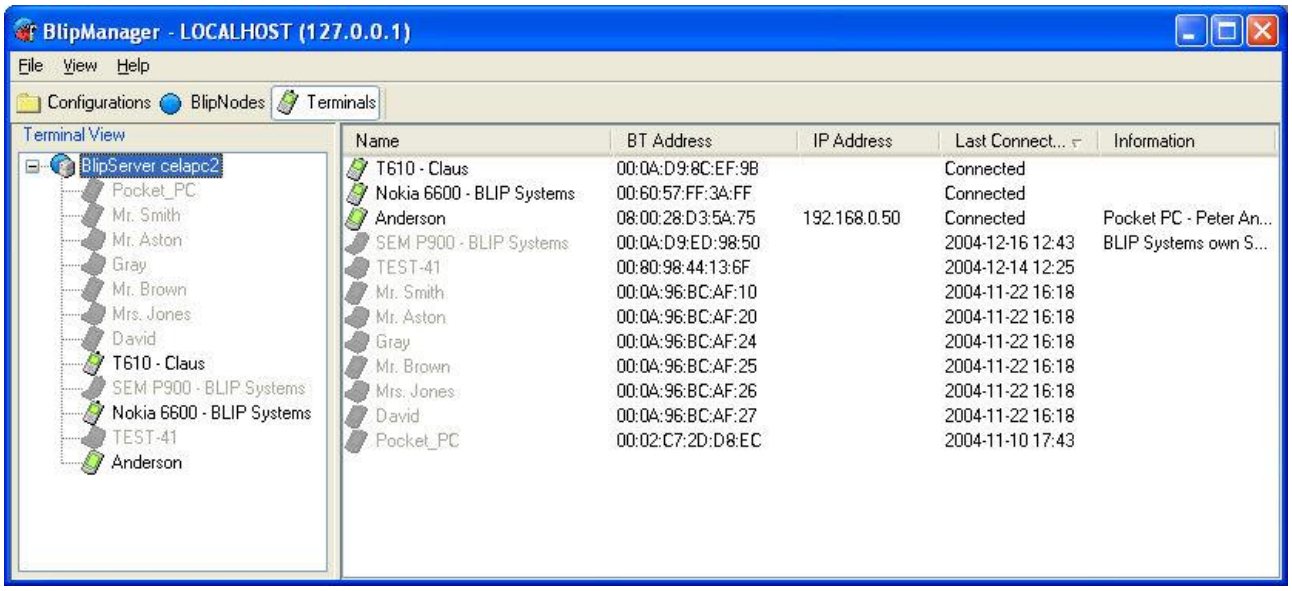
You can use Drag and Drop to specify the Topology of the Wireless BlipNodes.

1. Dropping a BlipNode on the BlipServer Icon makes the BlipNode an Ethernet BlipNode.
2. Dropping a BlipNode on another BlipNode makes the "dropped" BlipNode a Wireless BlipNode. The BlipNode will use a Bluetooth connection to the parent BlipNode in order to communicate with the BlipServer.

For more information about Wireless BlipNodes please read the chapter About Wireless BlipNnodes

Terminal View

The Terminal view displays all the Bluetooth Terminals that the BlipServer has registered in its database.

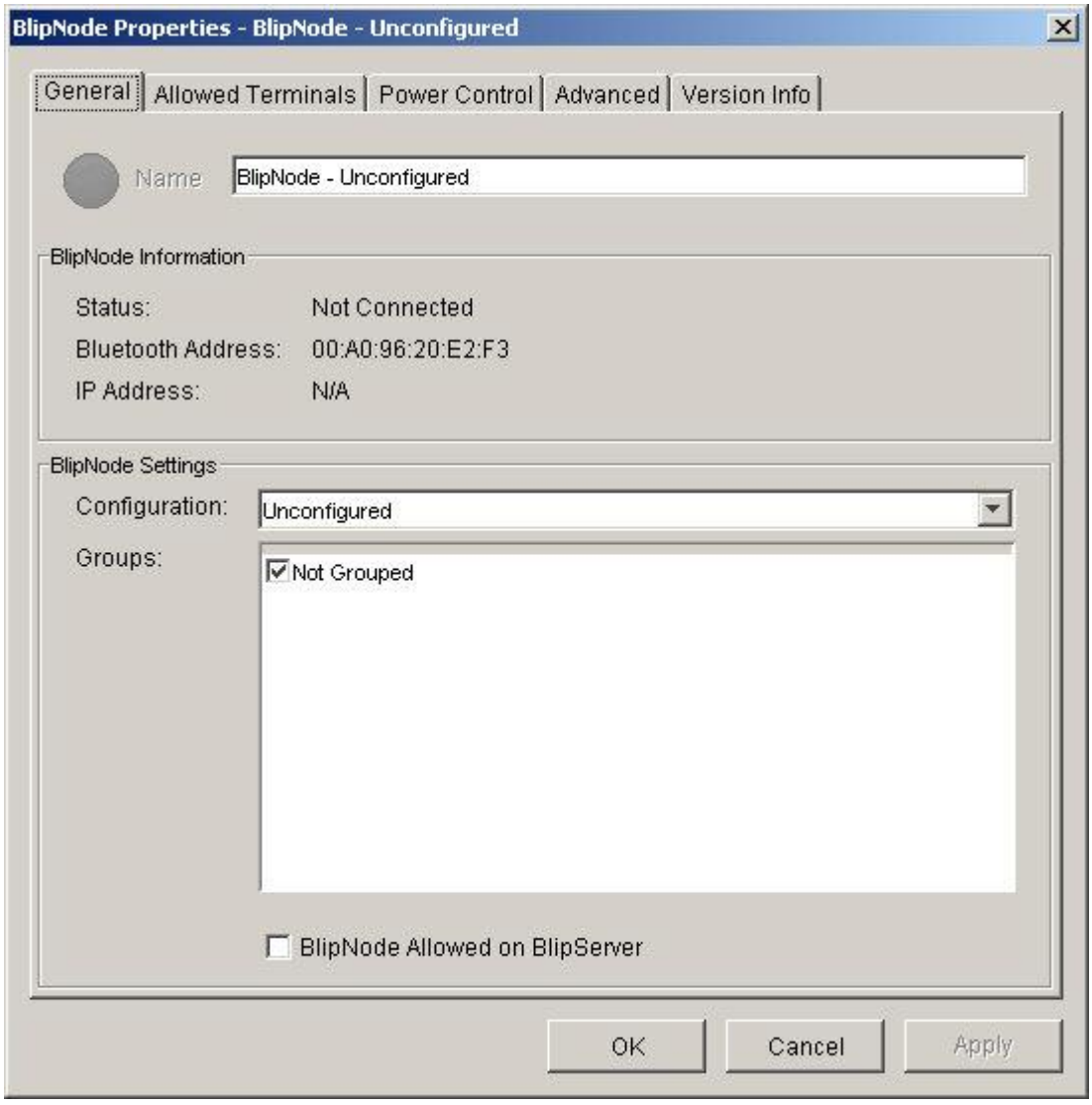


Terminals that are not currently connected to the BlipServer are presented with ghosted gray icon.
In the detailed pane you can choose to sort the terminals after Last Connected which gives you an easy way to monitor the connectivity of you terminal clients.

BlipNode Properties

General

In the General window in BlipNode Properties it is possible to configure the primary settings of a BlipNode. Additionally, information about the status, Bluetooth address, IP address of a BlipNode is displayed.



Name
The first text field contains the friendly name of the BlipNode. This is the name shown on the GUI on a connecting device.

Status
The status of the BlipNode. Status possibilities are; Not Connected, Connected, In use by application, Software upgrade in progress.

Bluetooth Address
The Bluetooth address of the BlipNode.

IP address
The IP address of the BlipNode. Automatically retrieved using DHCP.

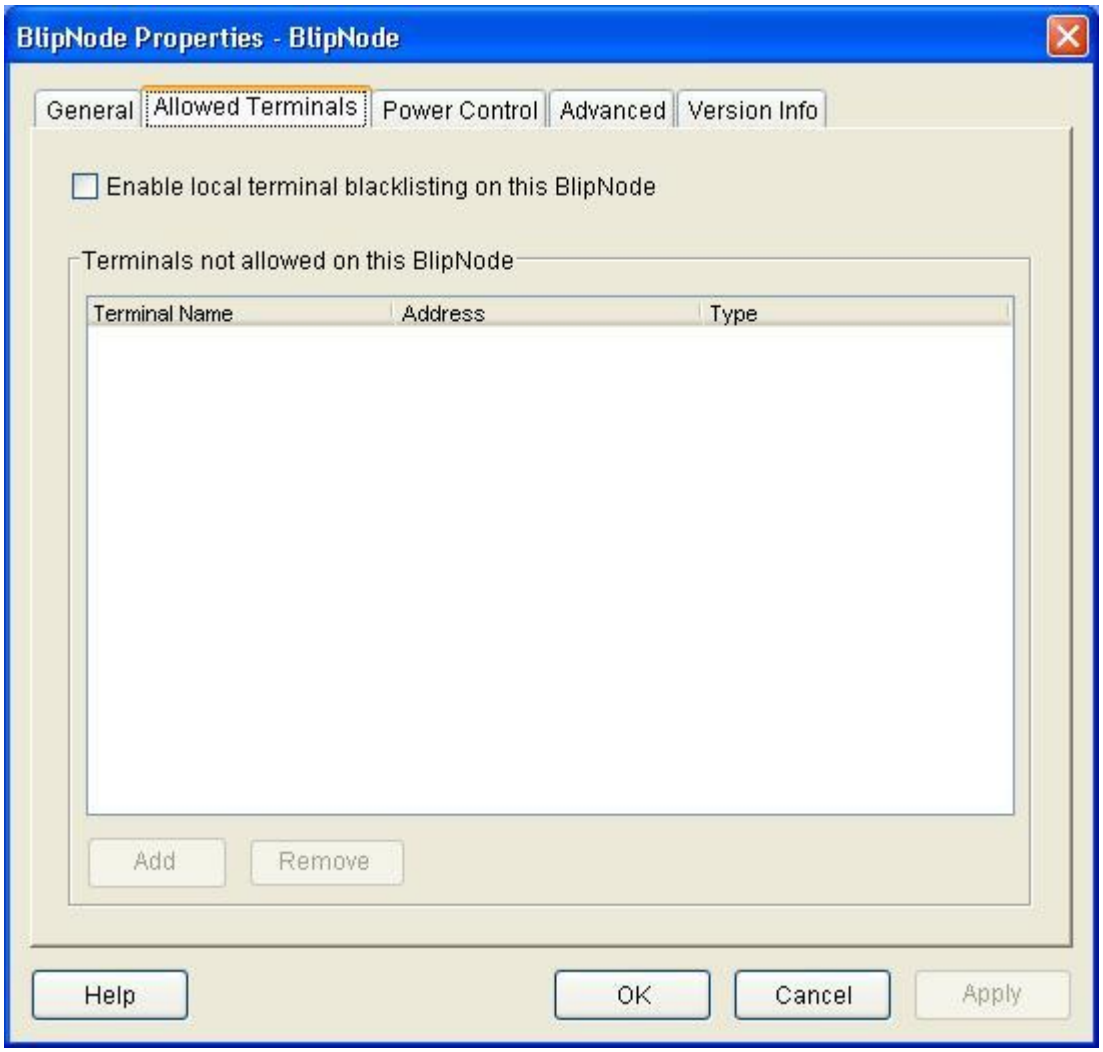
Configuration
In this list box the configuration of the BlipNode can be selected, see section General about BlipNode Configuration for further information.

Groups
This list shows the groups the BlipNode is a part of. The BlipNode can be inserted/removed from groups by clicking in the corresponding checkboxes. For a full description of the group concept please refer to section Using the BlipNode Groups Concept.

BlipNode Allowed on BlipServer
If checked on, the BlipNode is added to the Allowed BlipNode list in BlipServer Properties.

Allowed Terminals

In the Allowed Terminals window in BlipNode Properties it is possible to make a list containing terminals that are disallowed on the specific BlipNode.



If the checkbox "Enable local terminal blacklisting on this BlipNode" is unchecked all terminals will be allowed to connect. This is the default and recommended setting.

By checking this checkbox, terminals can be added to a disallowed list by clicking the "Add" button. These terminals will never be allowed to connect to this BlipNode regardless of the terminals setting in Terminals Panel in BlipServer Properties.

Power Control

In the Power Control window in BlipNode Properties it is possible to specify the power levels of the BlipNode.

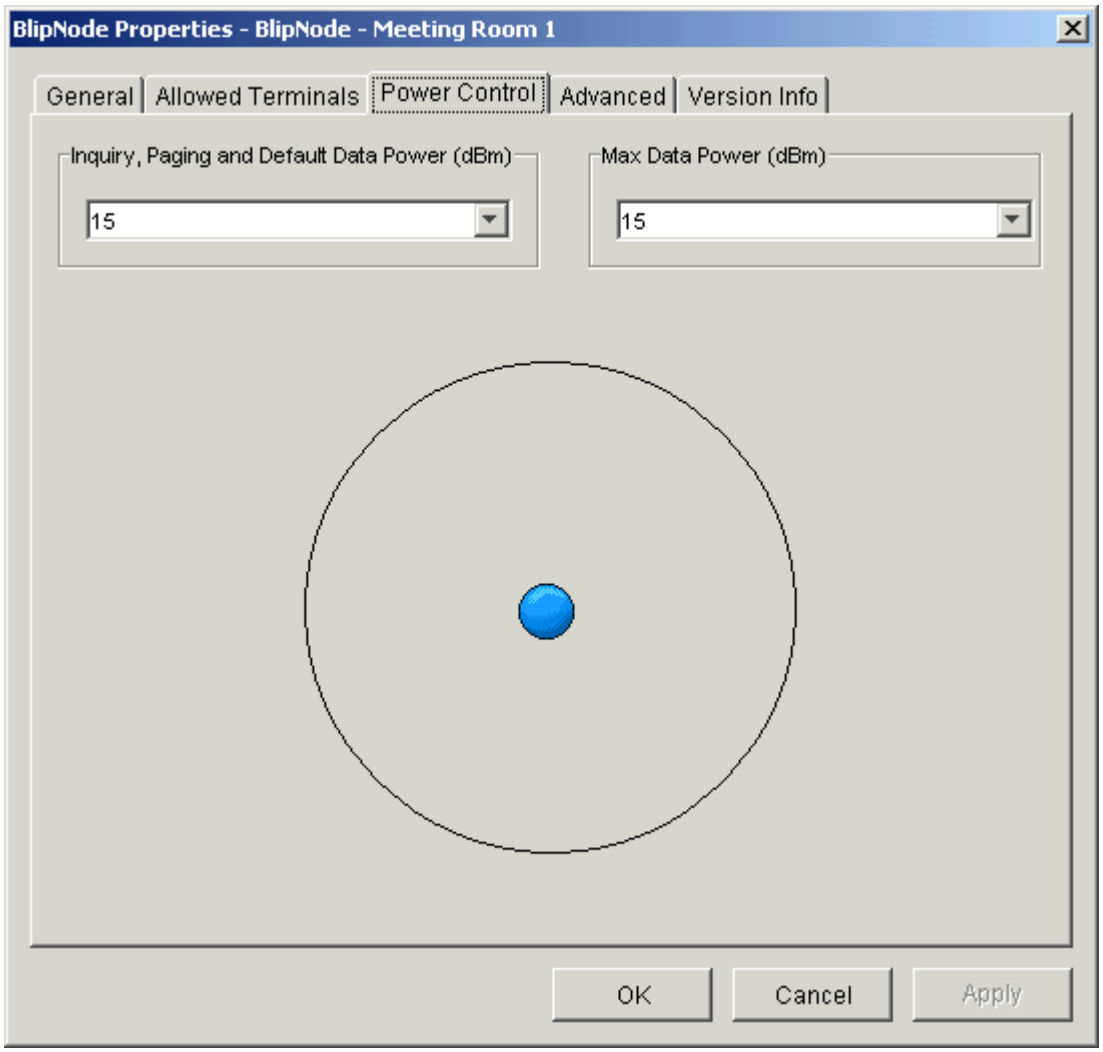
BlipNode requirements

Hardware	Power control is possible when using BlipNode L1 hardware, which is a power class 1 Bluetooth device (+20 dBm). Power control is not possible when using BlipNode S1 hardware or older, which are power class 2 Bluetooth devices (+4 dBm).
Software	BlipNode software version must be BlipNode_R3A or newer.

Power control in Bluetooth

Power control is required for power class 1 equipment. The power control is used for limiting the transmitted power over 0 dBm. Power control capability could be used for optimizing the power consumption and overall interference level. Equipment with power control capability optimizes the output power in a link by measuring a Radio Signal Strength Indicator (RSSI) and if the RSSI value differs too much from the preferred value of a Bluetooth device, it can request an increase or a decrease of the other device's data transmit power.

The power of the output of a Bluetooth device is normally specified in units of dBm. The dBm is an abbreviation used to represent power levels above or below 1 milliwatt. Negative dBm (-dBm) represents power levels below 1 milliwatt, and positive dBm (+dBm) represents power levels above 1 milliwatt. In other words, a dBm value is a specific amount of power; 0 dBm is equal to 1 milliwatt and +20 dBm is equal to 100 milliwatt.

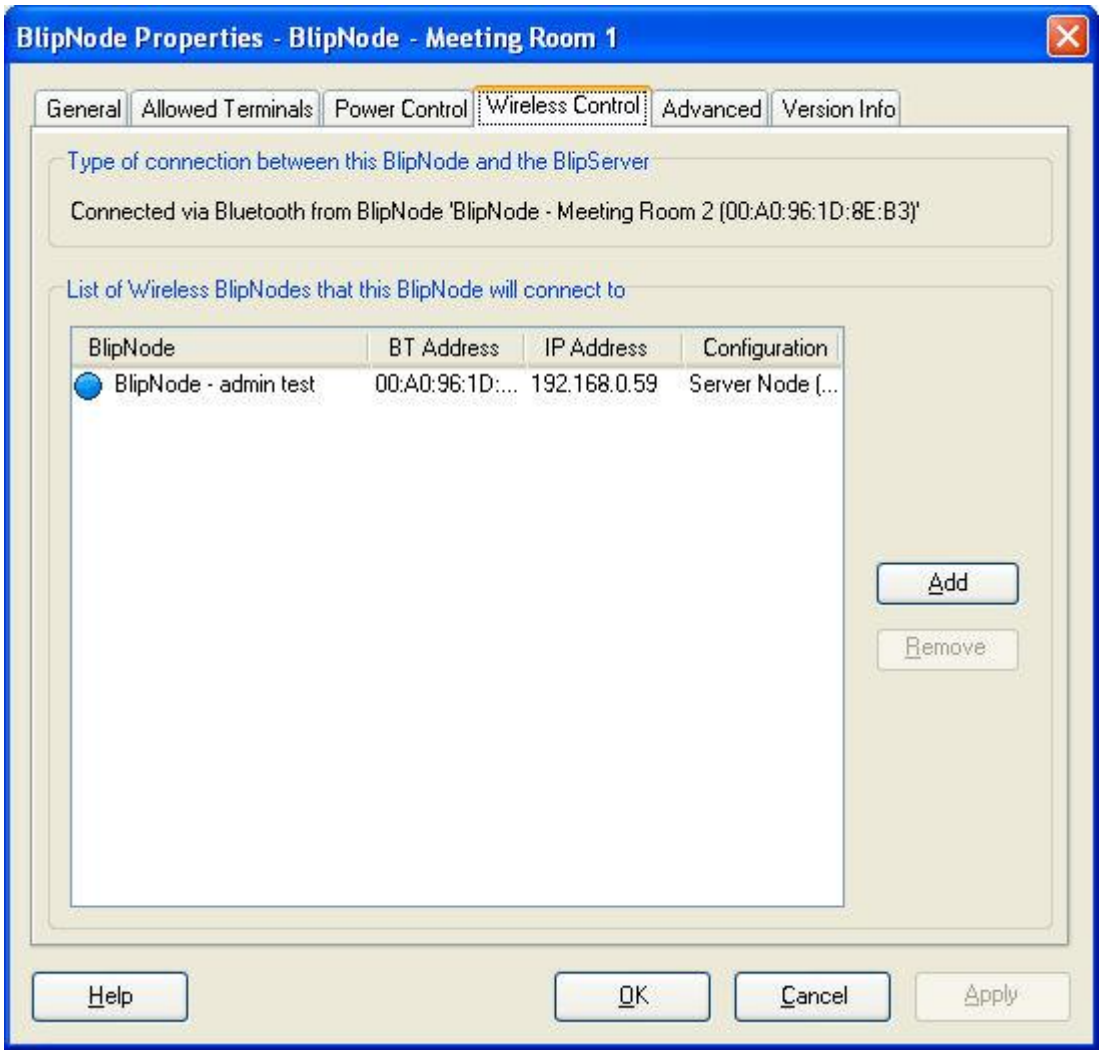


Inquiry, Paging and Default Power
This is the power level of the BlipNode used when transmitting. This means when making inquiry and paging. If a connected remote device has not increased or decreased the data transmit power, this power level also indicates the data transmit power.

Max Data Power
A connected remote device using power control can maximum increase the BlipNodes data transmit power to this power level.

Wireless Control

The wireless control pane allows you to monitor and configure the wireless properties of a BlipNode.



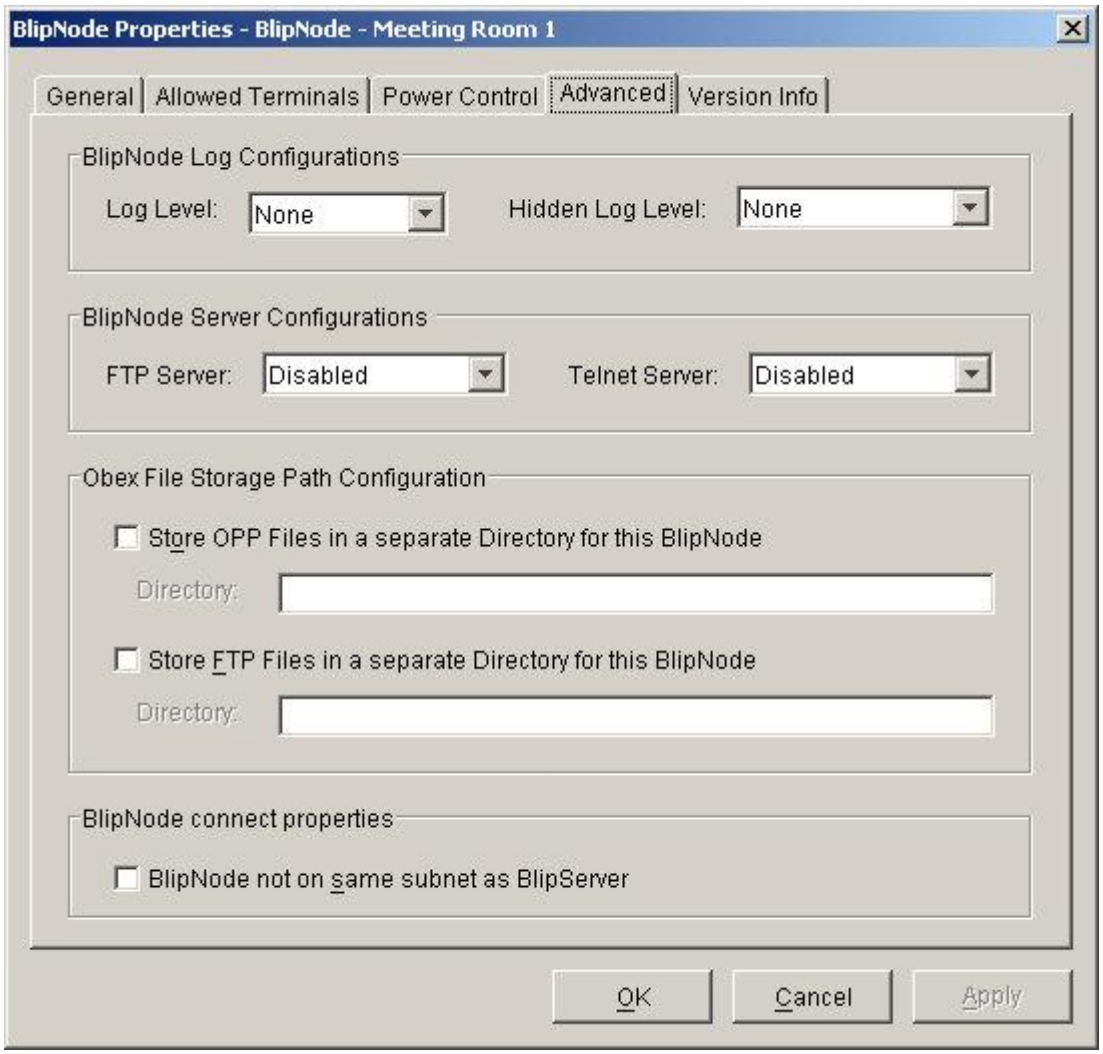
A wireless BlipNode is a BlipNode that is connected to the BlipServer through a Bluetooth Connection via other BlipNodes instead of using the Ethernet.

In this Windows it is possible to add a list of wireless BlipNodes that this BlipNodes that this BlipNode should connect to.

TIP. A more flexible way to configure wireless BlipNodes is by using Drag and Drop in the BlipManager BlipNode View. Please read section BlipNode View for more information.

Advanced

The Advanced window for a BlipNode contains a series of features that have been categorized as advanced features; normally a user will not need to change anything in this window.



BlipNode Log Configuration

The BlipNode has a built in log system. This feature has been made because it can improve the quality of our support in situations where a BlipNode fails to operate as expected. In this case the system can be used to generate a log file that can be sent to Ericsson Bluetooth Networks. The feature should not be used without contact to Bluetooth Network, since a PC application is required to receive the log via LAN. Normally there will be no need to make such log files.

Log Level:
Using this list box the log level of the BlipNode can be set. The level can be set to error, warning, info and trace. Trace is the most detailed level and this level shall be used when sending a trace to Ericsson Bluetooth Networks .

Hidden Log:

When enabled, trace will be stored in a buffer internally in the BlipNode.

BlipNode Server Configurations

The BlipNode has two servers running internally (FTP Server, Telnet Server). These servers are accessible via LAN only. A FTP server is used for the software upgrade. Default the FTP server is disabled and no software upgrade can be made. When the "Auto update of BlipNodes is enabled" the BlipServer will temporarily overrule this setting. A telnet server can be used for maintenance.

Obex File Storage Path Configuration

If the checkbox "Store OPP Files in a separate Directory for this BlipNode" is checked, files received via Object Push Server to this BlipNode, will be stored in the specified folder.

If the checkbox "Store FTP Files in a separate Directory for this BlipNode" is checked, the FTP Server root folder will the specified folder.

The entered directory/path will be created in the OPP/FTP file storage root path defined in the BlipServer properties window shown in section BlipServer Properties - Advanced.

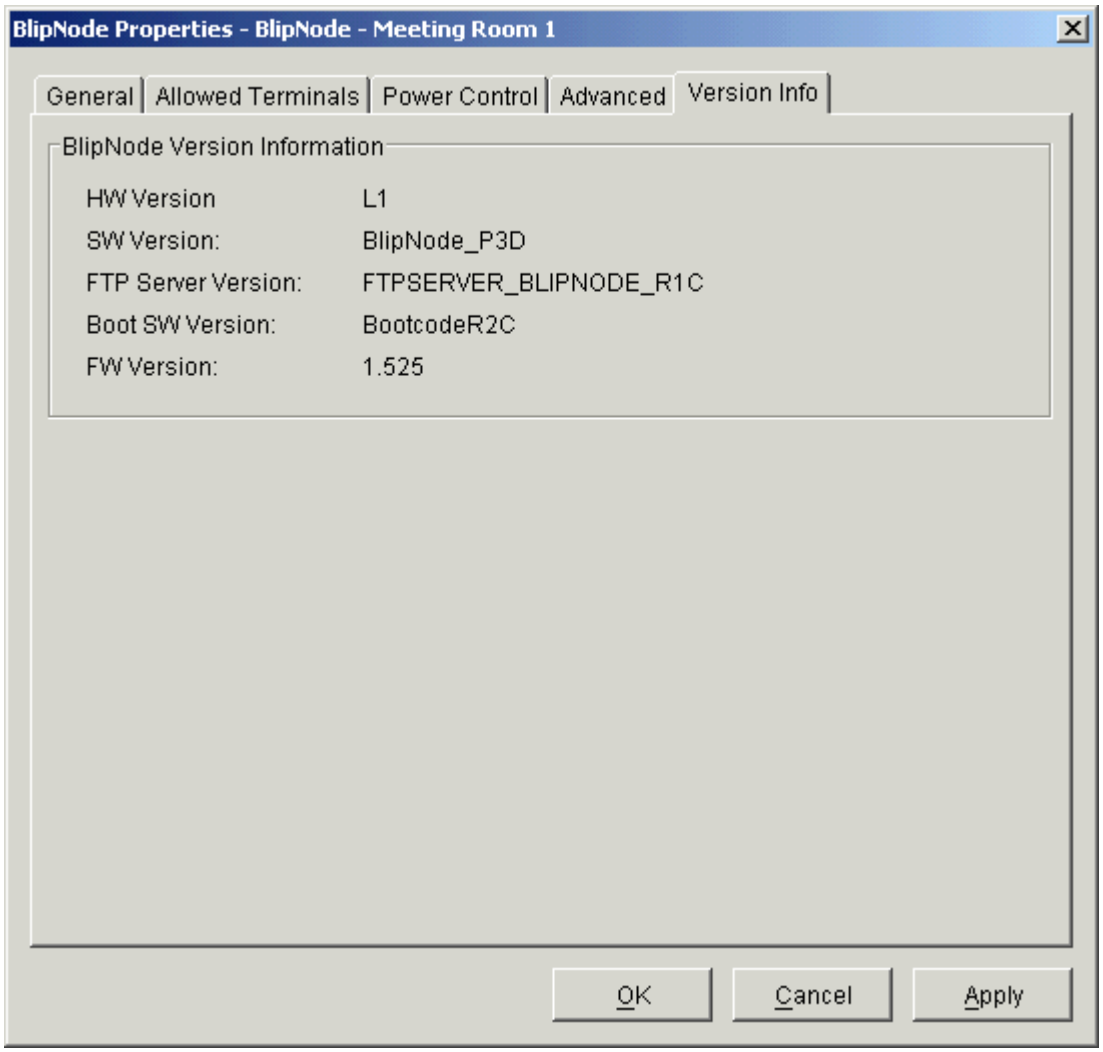
OPP Example on Linux:
BlipServer OPP File Storage Root Path: /opt/blipnet/Obex/OPP
BlipNode file storage directory: blipnode1
Received OPP objects on BlipNode1 will then be stored in following path:
/opt/blipnet/Obex/OPP/blipnode1

FTP Example on Windows:
BlipServer FTP File Storage Root Path: C:\Program Files\blipnet\Obex\FTP
BlipNode file storage directory: blipnode1
New FTP root Folder on BlipNode1 will then be the following path: C:\Program Files\blipnet\Obex\FTP\blipnode1

BlipNode not on same subnet as BlipServer
If enabled and a BlipServer IP address is specified in the BlipServer advanced Property sheet, the BlipNode will try to connect to the BlipServer IP address before sending out broadcast during the startup process. See also the BlipServer Properties - Advanced for more information on this topic.

Version Info

In the Version Info window in BlipNode Properties it is possible to see the hardware version of the BlipNode and the versions of the different software on the BlipNode.



HW Version
The hardware version of the BlipNode.

SW Version
The version of the application SW on the BlipNode.

FTP Server Version
The version of the FTP server SW on the BlipNode.

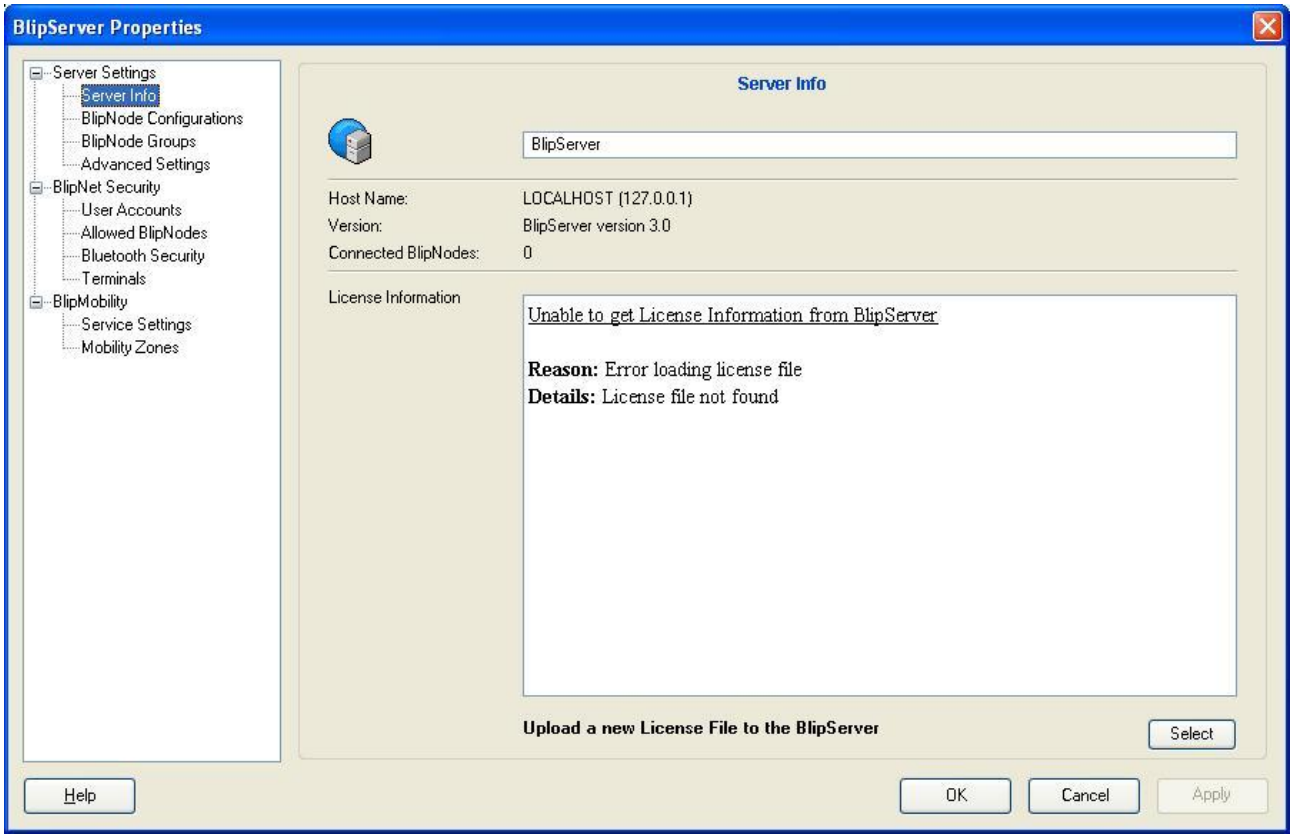
Boot SW Version
The version of the boot SW on the BlipNode.

FW Version
The SW version of the Bluetooth module Firm Ware on the BlipNode.

BlipServer Properties

Server Info

The BlipServer Properties - General window displays status and version information of the BlipServer.



BlipServer Name
In the text field at the top of the General window it is possible to enter the name of the BlipServer.

Host Name
The host name of the machine hosting the BlipServer. When running the BlipManager locally on the same machine as the BlipServer the host name is `localhost (127.0.0.1)`

Version
The version information includes version, release and build number of the BlipServer. The complete version information about all components in BlipNet can be seen by choosing About from the Help Menu.

BlipNode Licenses
The maximum possible number of simultaneously connected BlipNodes as specified in the license file.

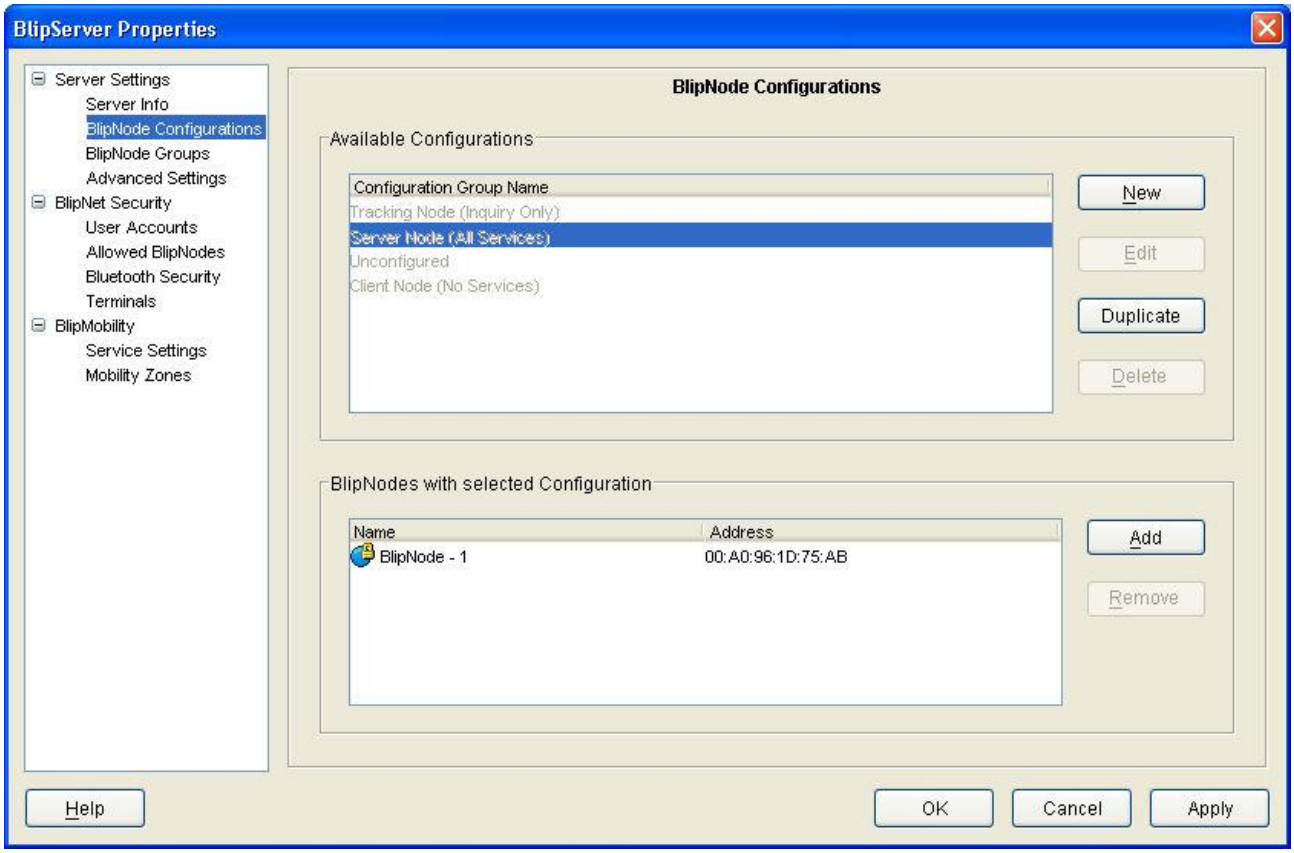
Connected BlipNodes

The actual number of connected BlipNodes on this BlipServer.

License Information
Displays information about your BlipNet License. If no valid license file is loaded on the BlipServer, the pane will display an error message shown above..
You can upload the license file you have received from BLIP Systems by clicking the Select Button and browse to your received license file.

BlipNode Configurations

Via the BlipNode Configurations window it is possible to define Configuration Groups and to assign BlipNodes to specific Configuration Groups. A Configuration Group is a set of BlipNodes sharing the same basic configuration. The BlipNodes do not share the exact same configuration. E.g. the friendly name can vary, and BlipNodes in the same Configuration Group does not necessarily have to belong to the same BlipNode Group.



The listbox with the title: "Available Configurations" contains a complete list of all Configuration Groups defined in the BlipServer. Some standard configurations are defined from manufactory side; these are grayed out in the list.

A description of the standard configurations can be seen in section General about BlipNode Configurations.

How to make new custom configurations is described in section Making a new BlipNode Configuration.

In the BlipNode Configuration window it is possible to:

- Add a new Configuration Group.
- Edit a Configuration Group.
- Duplicate a Configuration Group.
- Delete a Configuration Group.

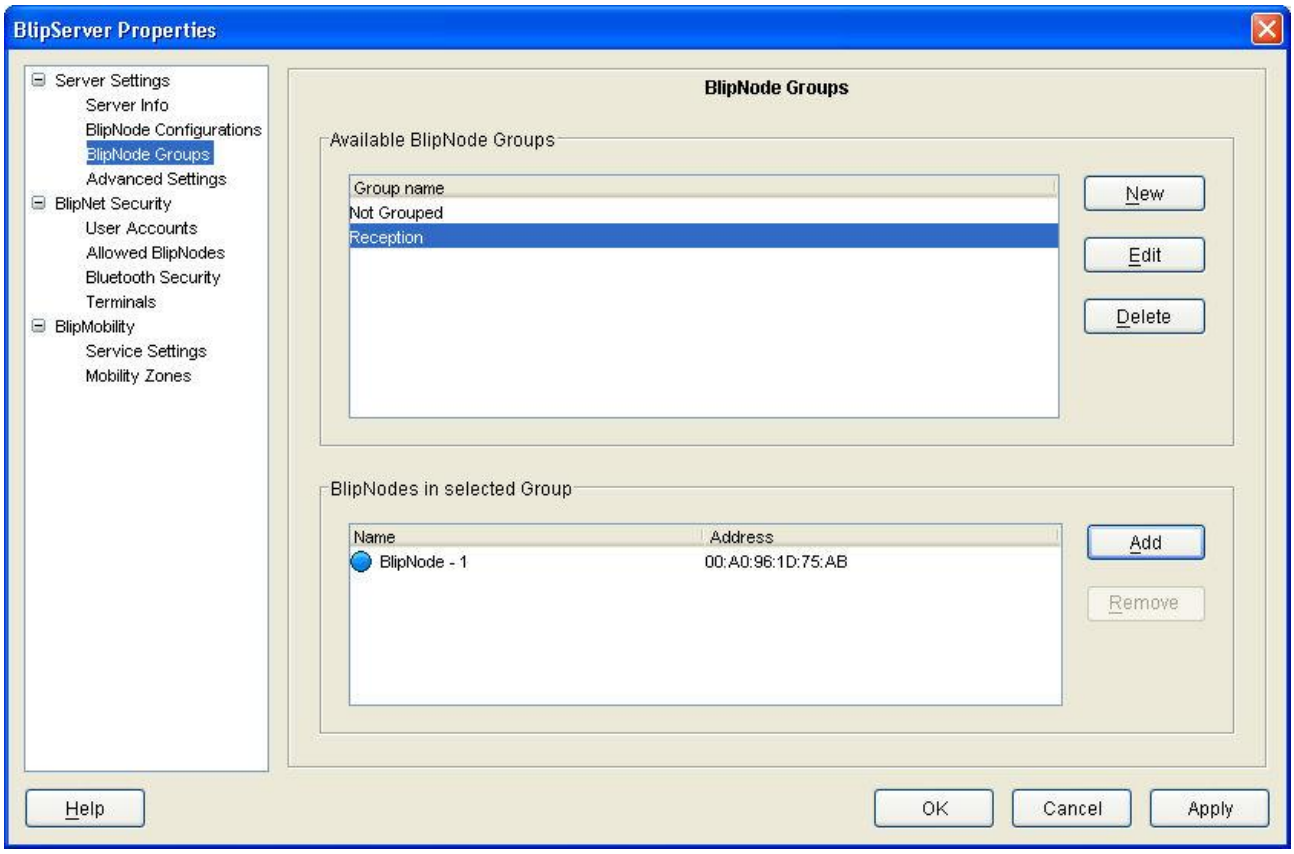
- Add BlipNodes to a specific Configuration Group.
- Remove BlipNodes from a specific Configuration Group.

A configuration wizard will help to guide you through the different configurations when trying to add a new, edit or duplicate a Configuration Group.

A BlipNode with no Configuration Group will automatically be assigned the "Unconfigured" group.

BlipNode Groups

A BlipNode Group is a logical name for a collection of BlipNodes. The BlipNodes in a BlipNode Group may have different configurations. A BlipNode Group name can for example be a location (e.g. "Reception") or an application Name (e.g. "Laptop Detector"). An application developer can use the BlipNode Group name to retrieve the BlipNodes assigned to this particular group from an application.



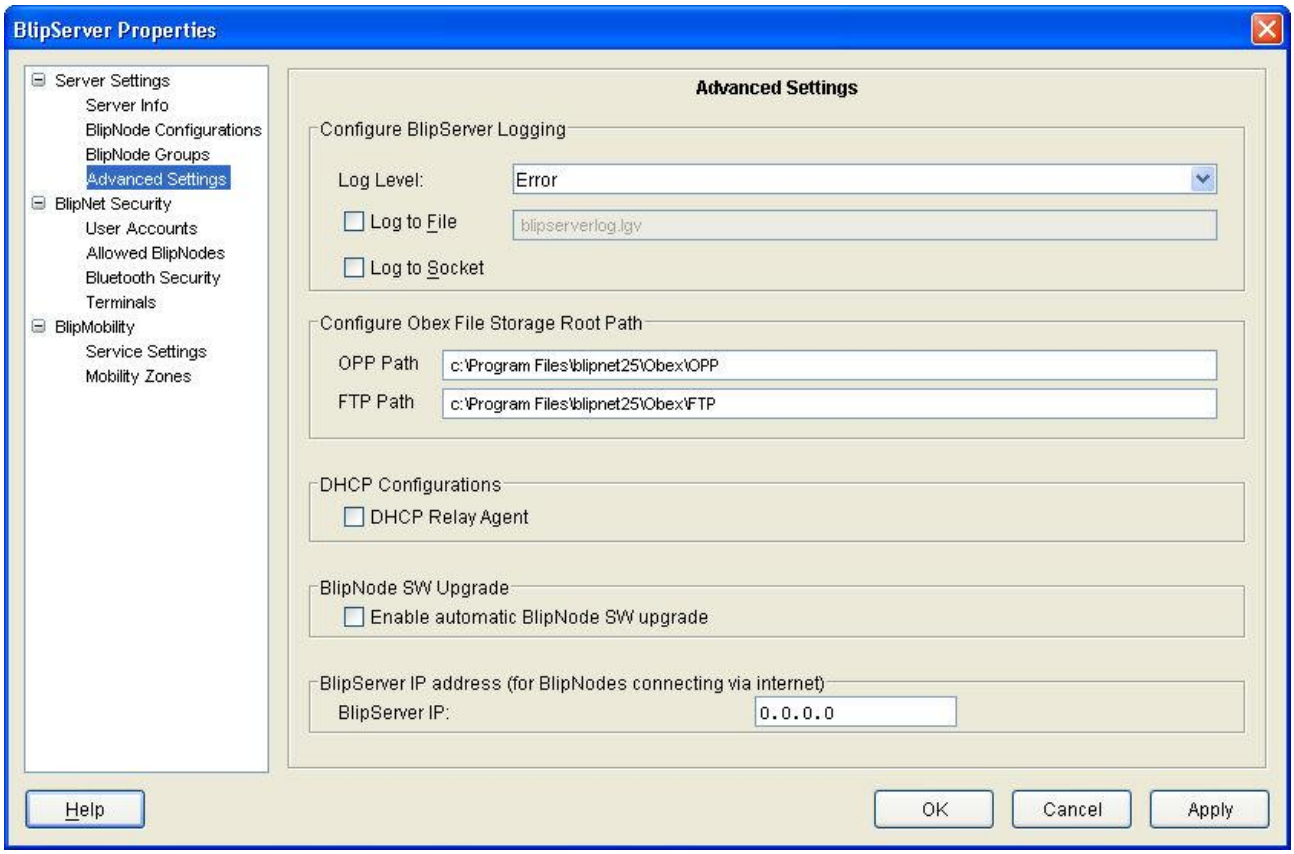
In the BlipNode Groups window it is possible to:

- Add a new BlipNode Group.
- Edit a BlipNode Group (this means changing the BlipNode Group name).
- Delete a BlipNode Group.
- Add BlipNodes to a specific BlipNode Group.
- Remove BlipNodes from a specific BlipNode Group.

The BlipNode Group name should be used in the application when searching for a BlipNode belonging to this group. BlipNodes, which are not added to any specific BlipNode Group, will automatically be added to the "Not Grouped" group. A BlipNode can be a part of more than one BlipNode Group at the same time.

Advanced

The BlipServer Advanced Settings contains a series of features, which usually not will have to be edited. The different settings in the BlipServer Advanced window are described below.



Configure BlipServer Logging

The BlipServer has a built in log system. This feature has been made because it can improve the quality of our support in situations where BlipNet application developers have problems using the BlipServer API. In this case the system can be used to generate a log file that can be sent to Ericsson Bluetooth Networks.

Normally there will be no need to make such log files.

Log Level:
Using this list box the log level of the BlipServer can be set. The level can be set to error, warning, info and trace. Trace is the most detailed level and this level should be used when sending a trace to Ericsson Bluetooth Networks.

Log to File:
If checked the system will log to a file with the specified file name.
IMPORTANT: There are no built-in restrictions on the size of the file. Switching on logging during long periods, especially at trace level, might result in a full hard drive, which will eventually cause the BlipNet to fail.

Log to Socket:
This feature enables Ericsson Bluetooth Networks to view logging information online. This checkbox should only be used in co-operation with Ericsson Bluetooth Networks.

Configure Obex File Storage Root Path

In these text fields the Obex storage root folders for the Object Push Profile (OPP) Server and File Transfer Profile (FTP) Server can be set. Default are all received OPP objects stored in the folder <blipnet installation dir>/obex/OPP and FTP files in <blipnet installation dir>/obex/FTP.

OPP Objects will be stored with the name "DeviceBlutoothAddress"_"ObjectName"."ext", for example "008037bc2123_MyCard.vcf". Objects will be overwritten if an object with the same name is received again.

Important
FTP Objects are stored without name change. Within the FTP root folder, FTP client users has unlimited rights to read, create and delete file and folders. As a result it is NOT recommended to specify a FTP root folder to sensitive data areas. I.e. a FTP root folder set to C:\ will give FTP clients unlimited access to your Server!

The BlipServer can sort objects based on the BlipNodes receiving the objects. This can be done by setting a specific storage folder on a BlipNode, see section BlipNode Properties - Advanced.

DHCP Configurations

When a terminal needs an IP-address the BlipNode retrieves this IP address from a DHCP server on behalf of the terminal. Normally the DHCP server distributes IP addresses using broadcast and in this case the relay-agent should be switched off. BlipNet 1.0 should be installed on top of a RedHat 7.2 installation. When using the DHCP server in this RedHat distribution the relay agent should be switched off. Certain DHCP server applies unicast and in this case the relay-agent should be switched on.

If a RedHat 6.2 DHCP server is used the DHCP relay agent should be switched ON.

BlipNode SW Upgrade

The BlipNode is upgradeable via the LAN interface. When upgrading your BlipNet installation new versions might include a new version of the BlipNode Software. By enabling automatic Software update it will be possible to get the BlipNodes Software upgraded with the latest version.

When receiving a new release the update procedure is like this:

1. Make sure all BlipNodes that requires an update are listed in the "Allowed BlipNodes" list. This is done in "BlipServer Properties Allowed BlipNodes" window. Check the "Enable automatic BlipNode SW upgrade" checkbox. All allowed BlipNodes on the BlipServer will then be updated when they are restarted.
2. Right click on a BlipNode in the configuration view tree and choose "Restart".
3. Do NOT power off the BlipNode or disconnect it from the LAN during the update procedure, which in some cases can take up to 10 minuets.
   When the BlipNode is being updated it is "grayed" in the tree, when the software upgrade is finalized and the BlipNode is active again it will change color back to "blue" again.

If you should have a version of the software older than BlipNode R1A (BlipNet 0.5), please contact BLIP Systems for specific upgrade information.

BlipServer IP Address

The IP address of the BlipServer which the BlipNodes will try to connect to.

When a BlipNode boots, it sends out a broadcast signal. The BlipServer will catch this signal a create a connection to the BlipNode for configuration a monitoring.

If the BlipServer is not able to receive the BlipNode broadcasts for some reason, e.g. the BlipNodes are placed on another subnet, behind a NAT-router, etc., it is possible to specify the IP address of the BlipServer in all the BlipNodes.
The BlipNode's will then first try to create a direct connection to the BlipServer on the specified address. If this fails the BlipNodes will do broadcast. An IP address of 0.0.0.0 will disable direct connection establishment in the BlipNodes.

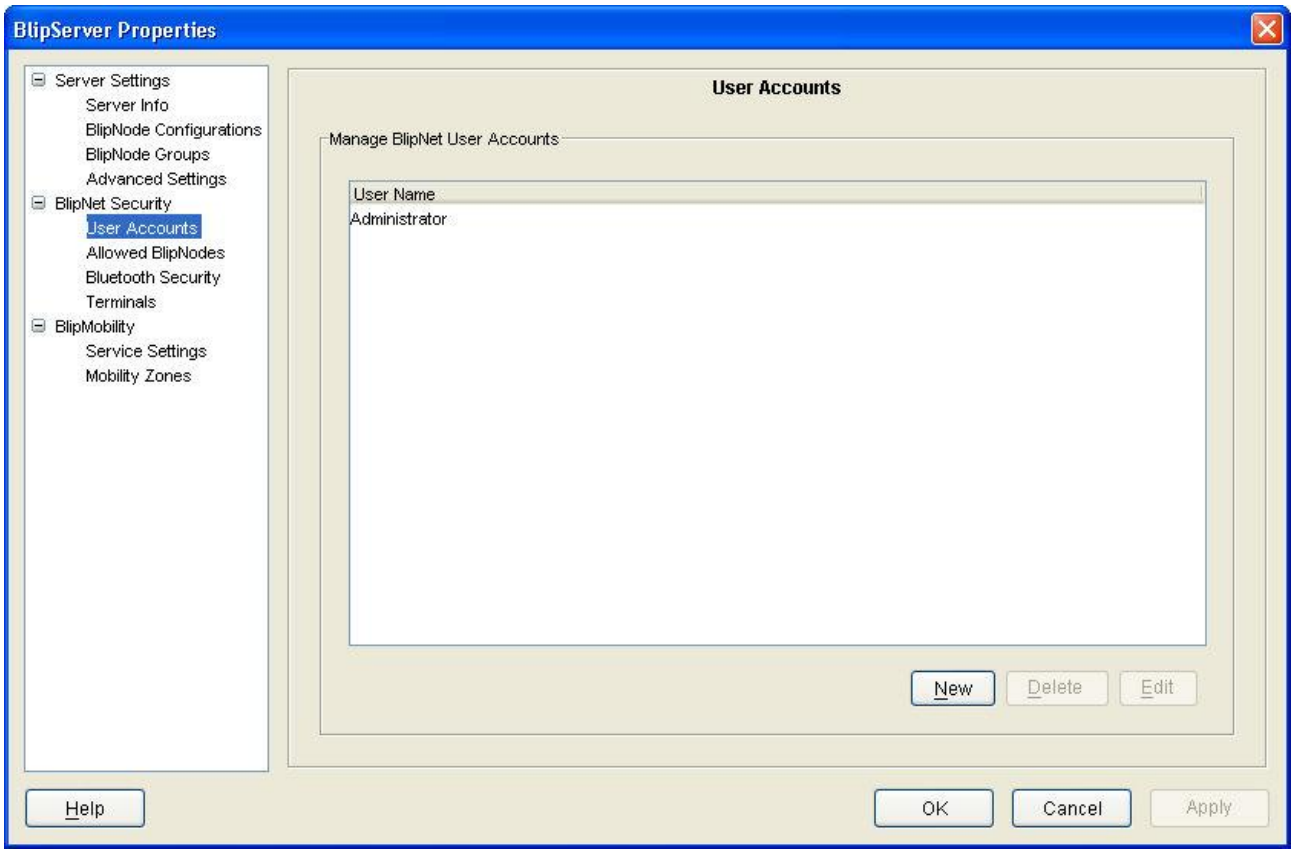
The BlipNode will only try to do a direct connection if the BlipNode is configured to be on another Subnet than the BlipServer.
You can enable/disable this for each BlipNode in the BlipNode Properties - Advanced Panel.

User Accounts

In the BlipServer Properties - User Accounts window everything about user accounts on the BlipServer can be configured. The BlipManager operates with the term "User account" at two levels. There is a user account for:

- The administrator
- Applications

To make it possible for an application to connect to the BlipServer a user account for the application must exist. An application can connect to the BlipServer using the credentials defined in this window (login and password). Howto connect an application to the BlipServer.



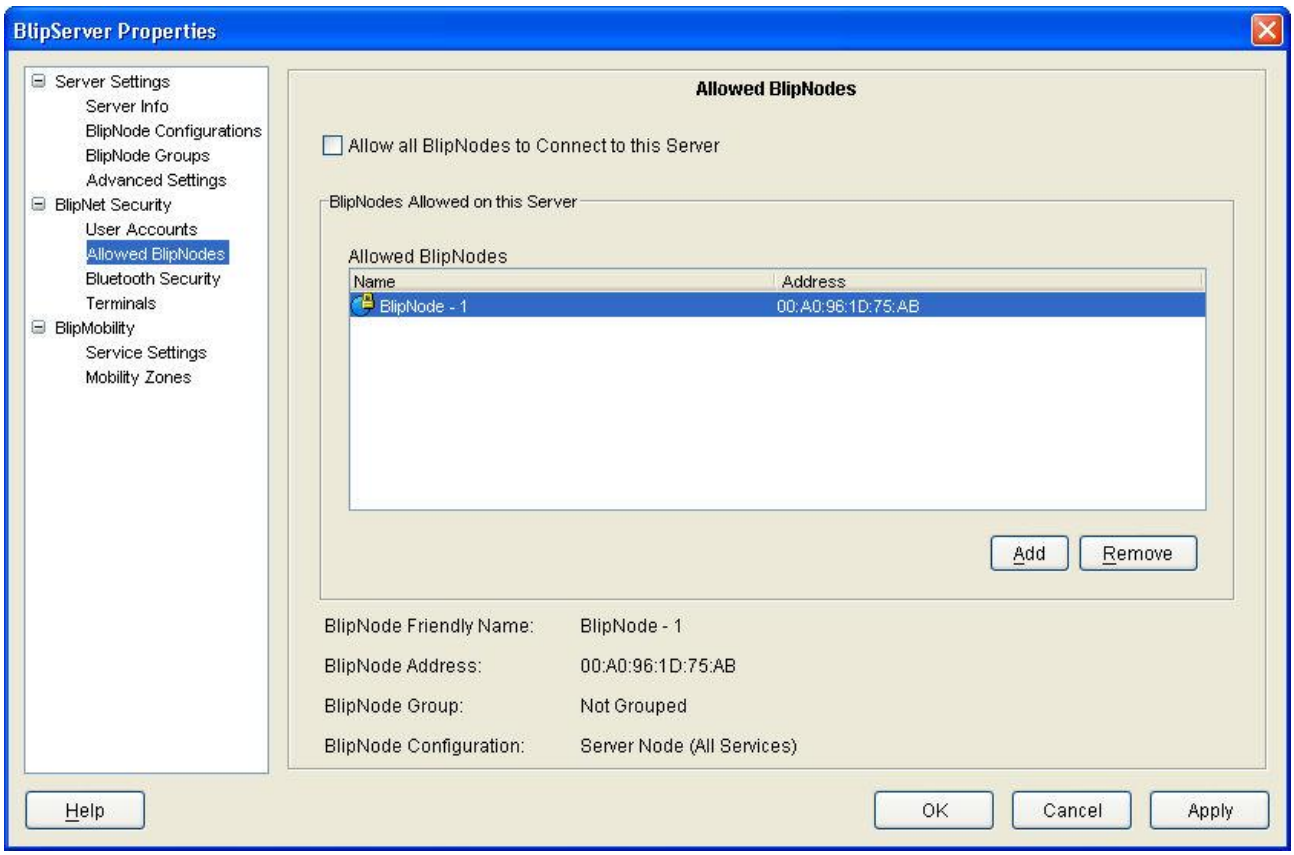
With the User Account settings it is possible to:

- Change the password for the Administrator.
- Add a new account.
- Delete accounts (this will prevent applications from connecting to the BlipServer).
- Edit accounts (this means change the password for a specific user account).

Allowed BlipNodes

From this window the allowed BlipNodes to connect to the BlipServer can be controlled.

The BlipNodes connects to the BlipServer via UDP broadcast and by default all BlipNodes will be allowed connection to the BlipServer. It can be desirable to have several BlipServers on the LAN. By specifying the allowed BlipNodes on the BlipServer, it can be controlled which BlipNodes that are allowed to connect to a certain BlipServer.



If the checkbox "Allow all BlipNodes to Connect to this Server" is checked, all BlipNodes can connect.

Security

Use the Security Settings to control the access to the BlipNet System. The Bluetooth passkey is the PIN code a user will have to use to make a secure relation between the users Bluetooth device and BlipNet. The creation of this secure relation is called “Pairing” or “Bonding”.

A Bluetooth device shall be either in non-bondable mode or in bondable mode. In bondable mode the Bluetooth device accepts paring – i.e. creation of bonds – initiated by the remote device, and in non-bondable mode it does not.

Via the BlipManager it is possible to define a default Bluetooth Passkey and Bluetooth Passkeys for specific terminals. If a terminal specific Bluetooth Passkey has not been defined, then a terminal must use the default Bluetooth Passkey when pairing with BlipNet. Otherwise, the specific terminal Bluetooth Passkey overrules the default Bluetooth Passkey.

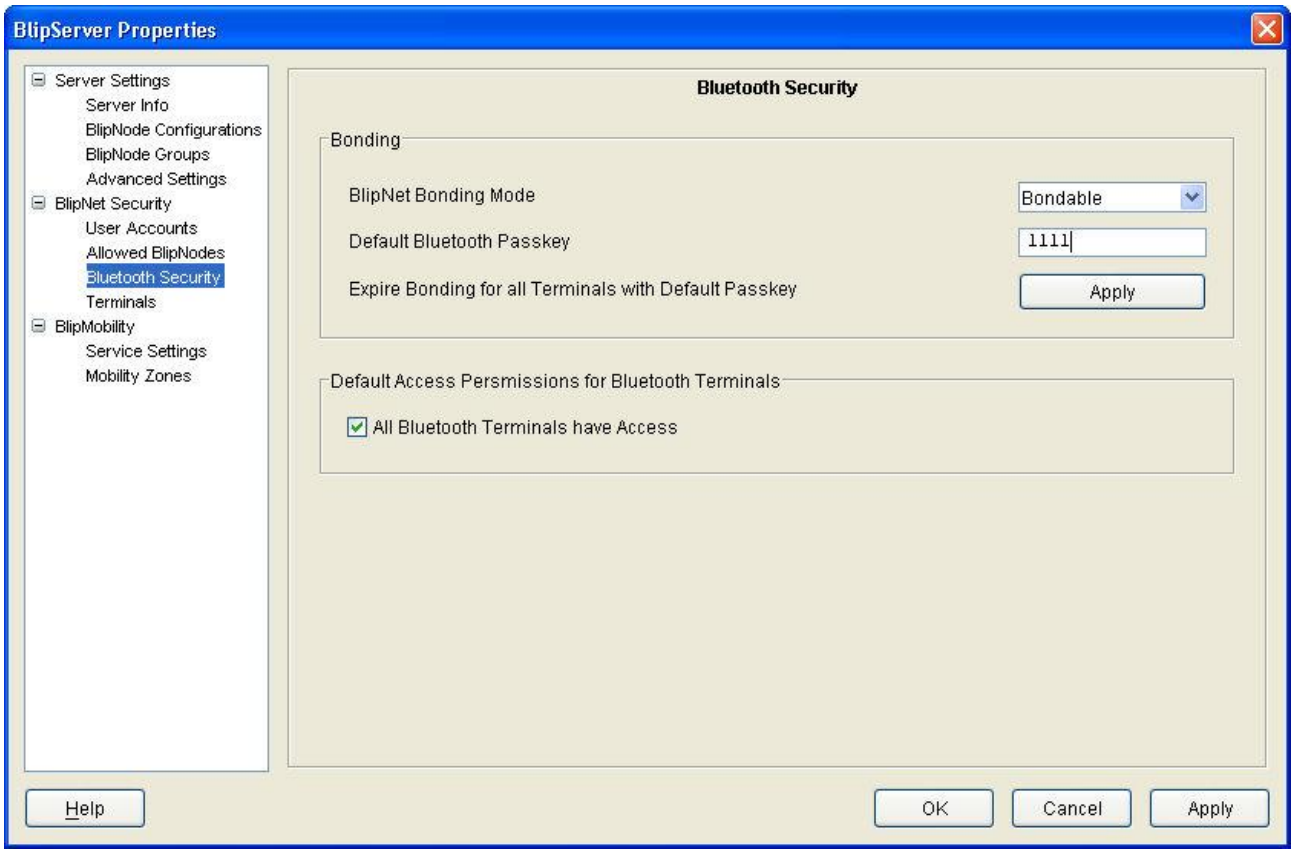
When connecting a Bluetooth device to BlipNet it will have to pair in following situations:

- Security level is “Link level” and the device is not already paired with BlipNet.
- Security level is “Service level”, the user tries to connect to a service with the checkbox “Require Authentication” checked, e.g. LAN access, and the device is not already paired with BlipNet.

“Link level” security is not used in any of the standard configurations.

When using the standard configuration "Server Node (All Services)", authentication is required when accessing the LAN Access, PAN Service or FTP Service, but not the OPP Server Service.

There is no limitation to the number of paired Bluetooth terminals that BlipNet can handle.

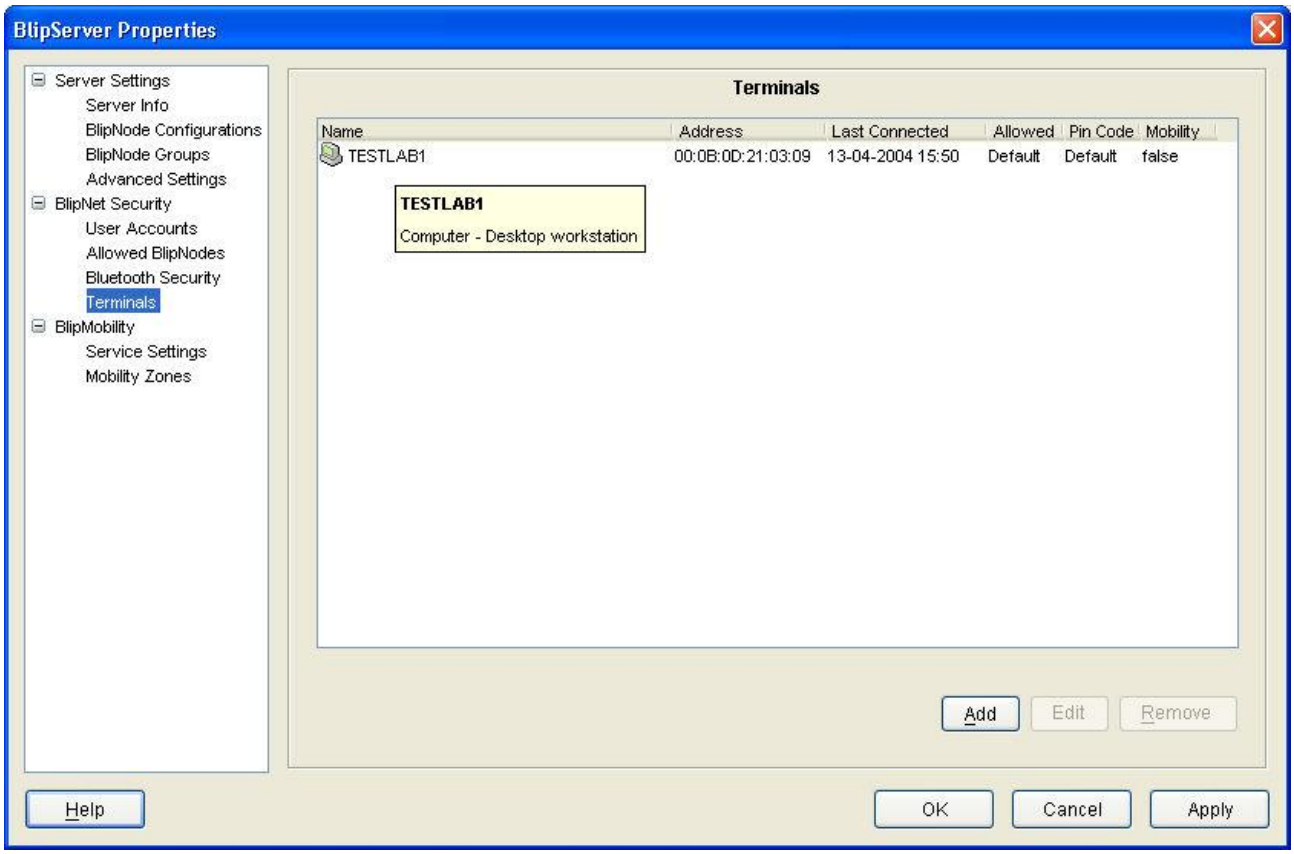


In the security window of BlipServer Properties it is also possible to expire Bluetooth bondings. When applying "Expire Bluetooth bonding on all devices" all "bonds" created by the default Bluetooth Passkey will be deleted. To delete the bonding to a terminal with a specific Bluetooth Passkey, the Bluetooth Passkey for the specific terminal must be deleted.

When switching from bondable mode to non-bondable mode this will not delete the existing "bonds" but new terminals are not allowed to bond with the BlipNet system.

Terminals

Use the Terminals window to control the terminals on the BlipServer.



This window displays all the Bluetooth terminals known by the BlipServer.
When a Bluetooth connection is established between a BlipNode and a Terminal it will automatically be added to this list.

The List shows the following information for each Terminal:

- Name — The last known Bluetooth Friendly name of the terminal.
- Address — The Bluetooth Address
- Last Connected — Shows either
  1. Connected: Currently Connected
  2. Date: Last time the Device had a Bluetooth Connection to the Server
  3. Never: The Terminal has never had a Bluetooth connection to a BlipNode
- Allowed — Shows the Connection Policy for a Terminal.
  1. Always: The Terminal is always allowed to connect to the BlipServer.
  2. Default: Depends on the System default setting in BlipServer Properties -> Bluetooth Security.
     Only if "All Bluetooth Terminals have Access" is enabled, the terminal will be allowed to connect.

3. Never: A Bluetooth connection can never be established between this terminal and a BlipNode.

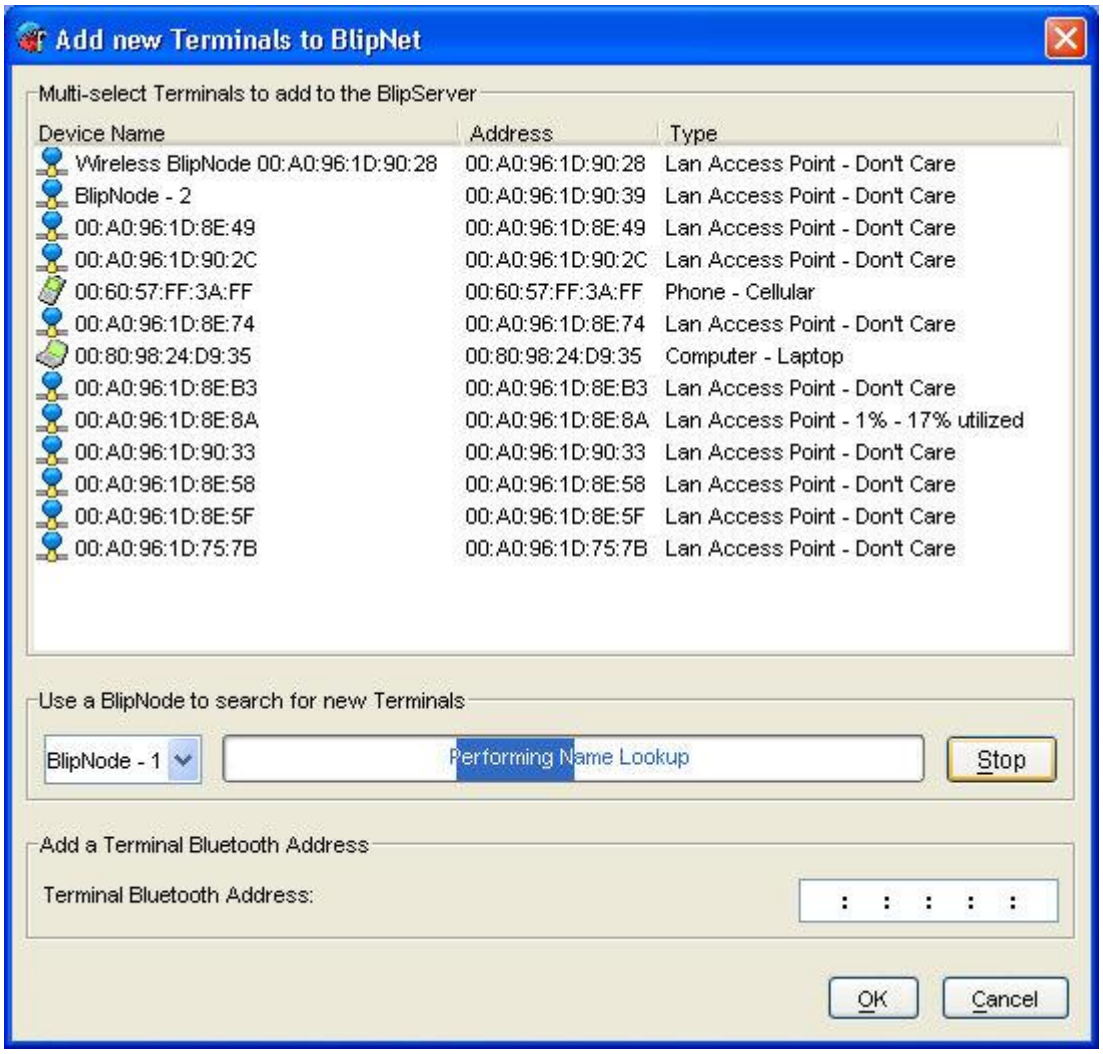
Note1: This policy is applied both when the terminal is establishing the connection and when connection is being established from the BlipNet API.
Note2: This Policy is independent of the Bluetooth Passkey settings. If a Pairing is needed and a wrong PIN Code is specified, the transaction will fail.

- Pin Code — Specifies the Bluetooth Passkey. This can be either "Default" which refers to the Default Passkey specified in BlipServer Properties -> Bluetooth Security, or a specific Passkey for this terminal only.
- Mobility — Specifies if this terminal is subscribed to the BlipNet PAN Mobility Service

Add

You can add new terminals to BlipNet in two ways:

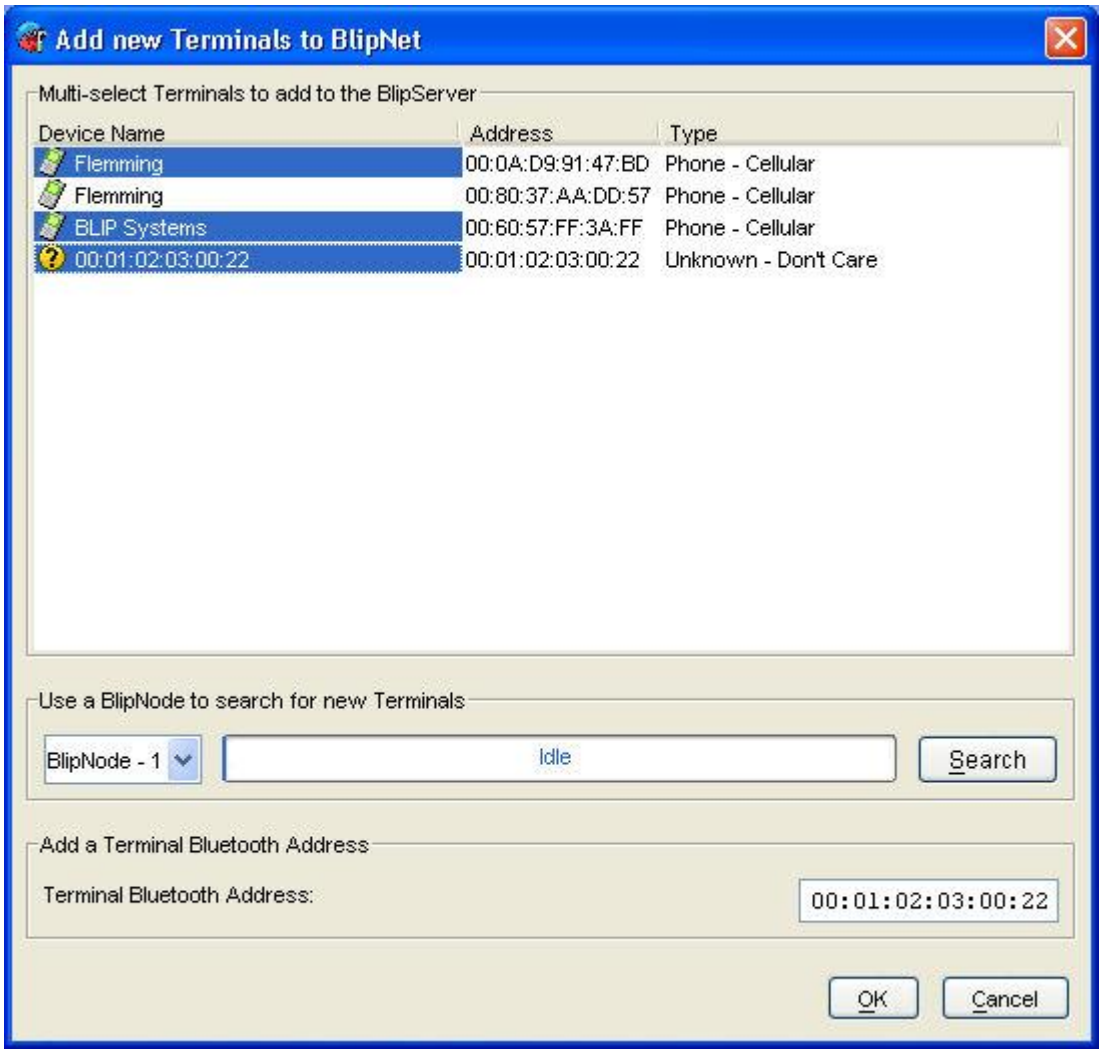
1. If BlipNet has been open to allow all Bluetooth terminals, you can set-up a Bluetooth connection from your Bluetooth device towards BlipNet. The terminal will automatically be added in the list.
2. Pressing the Add Button will bring up a Dialog to add new terminals.



The dialog gives two methods for adding terminals to BlipNet.:

1. Search for Bluetooth terminals by selecting a BlipNode and Press Search. The Results will be shown in the list.
2. Manually enter Terminal Bluetooth Addresses in Address Field. The Entered addresses will be shown in the list.

To add Terminals, multi-select the terminals from the window that you want to add then press the OK button.



Remove

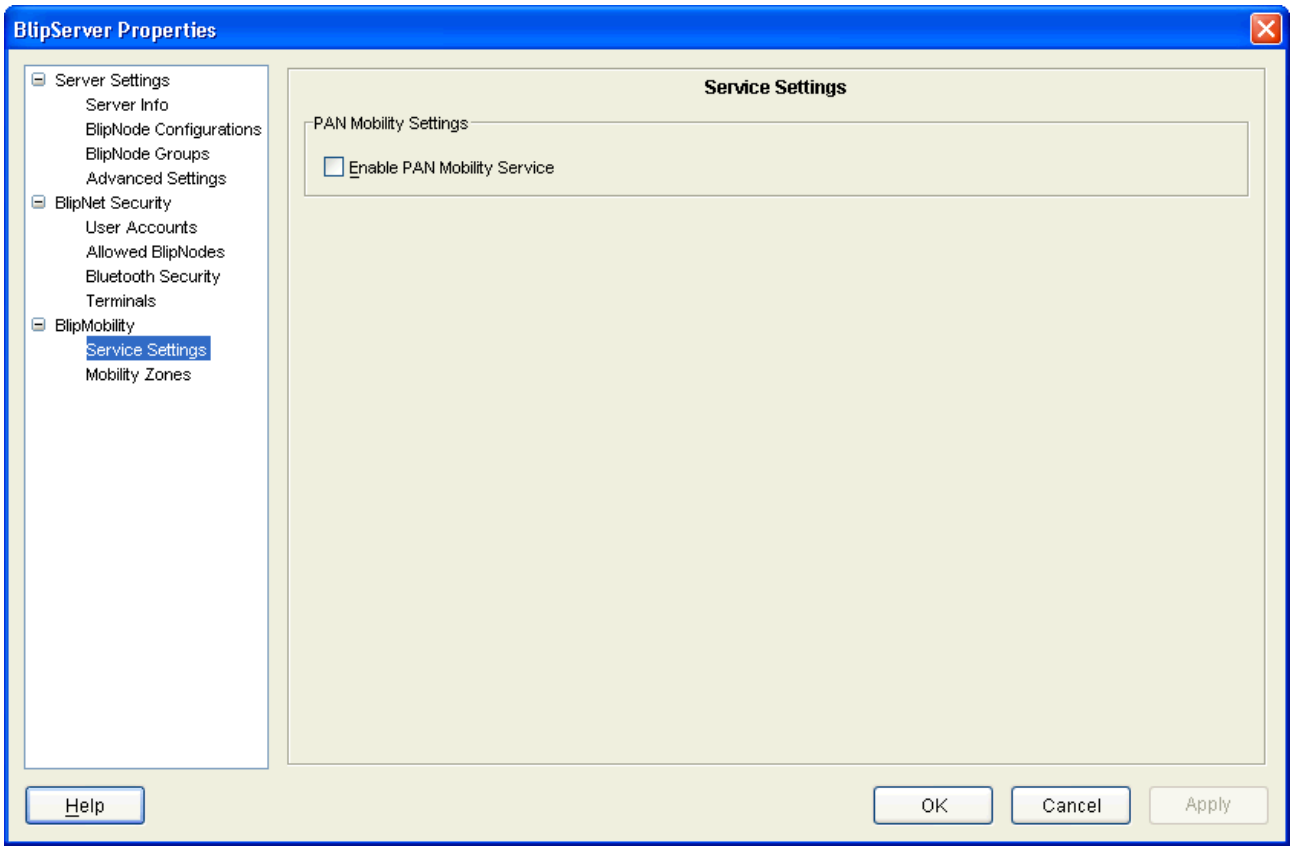
Pressing the Remove Button will delete the Selected Terminals from the System including all information like description and PIN Code.

Edit

The Edit Button will bring up a Dialog showing the Terminal Properties.

Mobility Settings

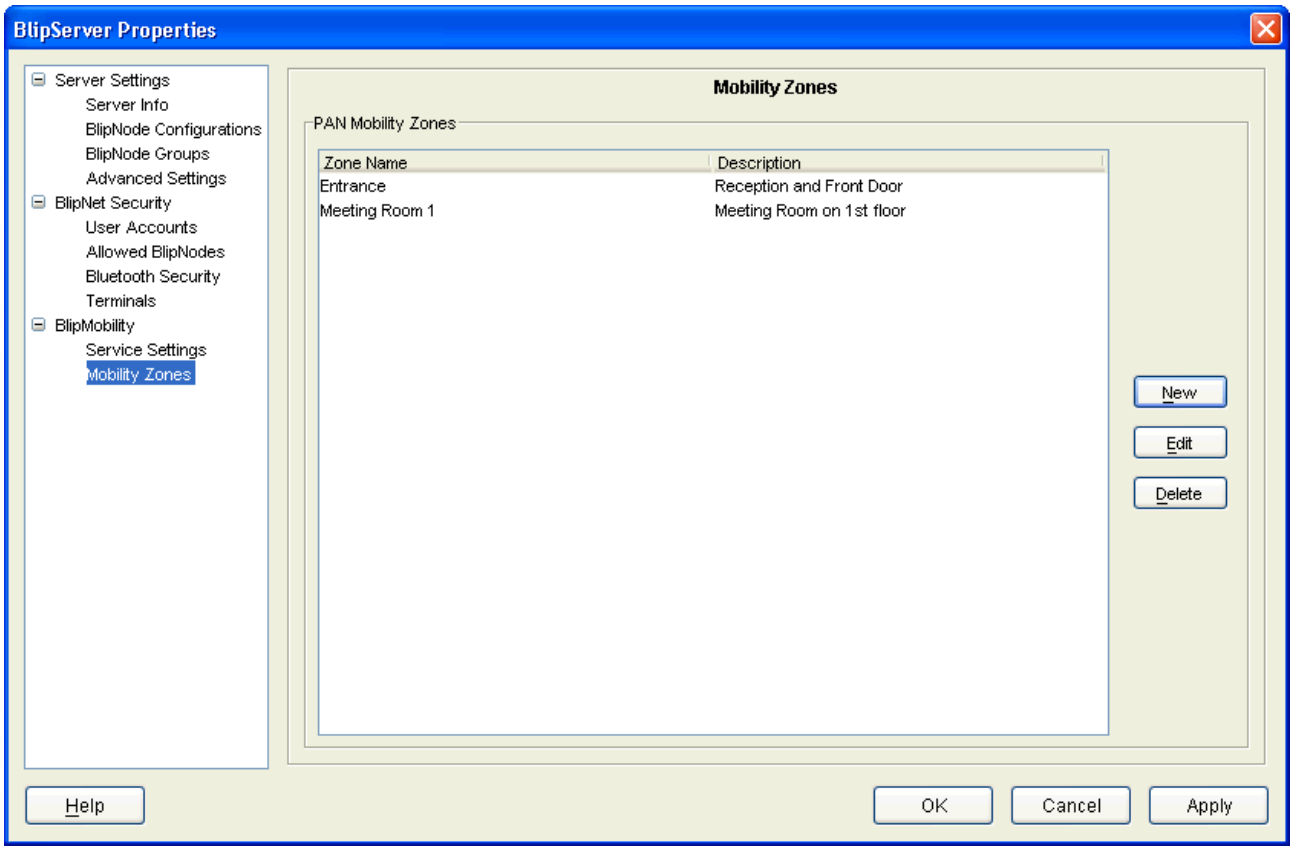
Here it is possible to enable or disable the BlipNet Mobility Service.



Before enabling this Service please read the Chapter BlipNet Mobility Service

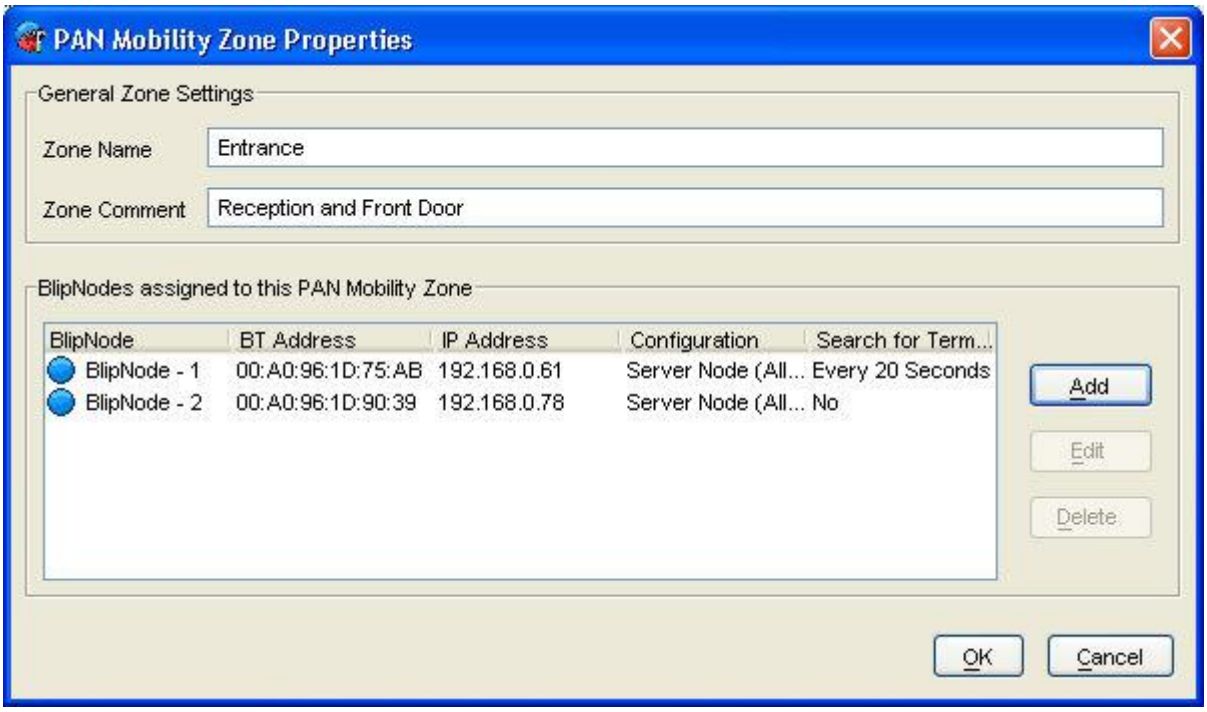
Mobility Zones

This page allows you to configure the BlipNet Mobility Zones. Please read BlipNet Mobility Service for general introduction to this Service.



The Window lists the created Mobility Zones.

Creating a new or editing an existing zone will bring up the PAN Mobility Zone Properties:

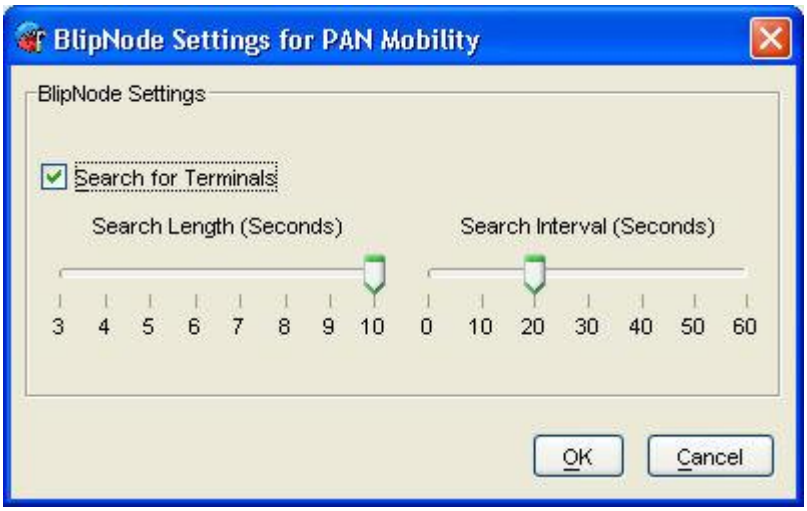


The Zone Name and Zone Comment defines the name of the Zone. A good idea is to specify a physical location. This makes it easy to determine the locations of connected terminals in the BlipManager tree view.

To each zone it is possible to assign a number of BlipNodes. Normally you would only have one BlipNode in each Zone, but if you have high penetration of Bluetooth devices or the need for more bandwidth to each device in a Zone you can add extra BlipNodes. The BlipServer will automatically do load balancing between BlipNodes in a Zone so terminal connections are equally distributed between the BlipNodes.

In each Zone one BlipNode must periodically search for terminals. The BlipServer uses this information to establish links to new terminals just powered on and to find hand over candidate zones.

While a BlipNode is searching for terminals the bandwidth to the connected terminals will be decreased. It is possible to change the search interval for each BlipNode by pressing the edit button:

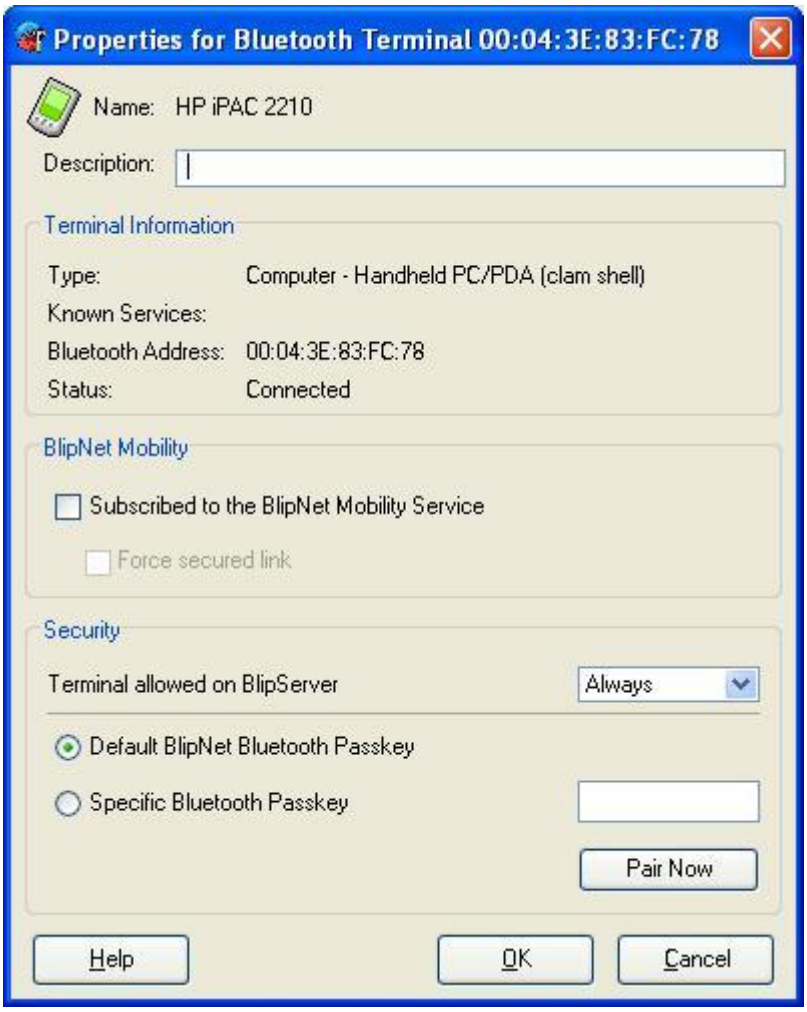


If the Search interval is very high it will take longer time for a newly powered on device to be connected and also the handover process will take more time because the BlipServer will not do the hand over to a BlipNode in a new Zone before the Terminal has been discovered in that Zone.

Terminal Properties

General

The Page shows information about the selected Bluetooth Terminal.



BlipNet Mobility

Specify here if this terminal is subscribed to the BlipNet Mobility Service. To use this service, the terminal must support the Bluetooth PAN Profile. For more information please read BlipServer Properties -> Mobility Service.

By enabling "Force Secured link", the BlipServer will make sure that the PAN Connection is always authenticated and encrypted, even if this has been disabled on the Terminal.
If it's not possible to specify a Default Passkey on the Terminal, the user will be prompted the first time Terminal is handed over to a new BlipNode.

Security

Terminal allowed on BlipServer:

1. Always: The Terminal is always allowed to connect to the BlipServer.
2. Default: Depends on the System default setting in BlipServer Properties -> Bluetooth Security.
   Only if "All Bluetooth Terminals have Access" is enabled, the terminal will be allowed to connect.
3. Never: A Bluetooth connection can never be established between this terminal and a BlipNode.

Note1: This policy is applied both when the terminal is establishing the connection and when connection is being established from the BlipNet API.
Note2: This Policy is independent of the Bluetooth Passkey settings. If a Pairing is needed and a wrong PIN Code is specified, the transaction will fail.

Passkey:

Gives the possibility to use the Default Bluetooth Passkey specified in BlipServer Properties -> Bluetooth Security or to specify a Passkey unique for this Terminal.

Pair Now

By clicking this button you can Pair the selected Bluetooth Terminal with a BlipNode of your choice. The Terminal must be Connectable and in range of the BlipNode that you choose to pair with.

BlipNode Configurations

General about BlipNode Configurations

Using the BlipManager it is possible to assign BlipNodes to a BlipNode Configuration. It is possible to specify such a BlipNode Configuration using a configuration wizard. For more information about the configuration wizard see section Making a new BlipNode Configuration.

The BlipManager has a set of pre-defined standard configurations. They are:

- Tracking Node (Inquiry Only)
- Client Node (No Services)
- Server Node (All Services)
- Unconfigured

The pre-defined standard configurations will now be explained in the following.

Client Node

The pre-defined Client Node configuration includes no services (Except the PAN service which is required for outgoing PAN connections). It is useable in cases where the BlipNode initiates the link establishment and no incoming connections are wanted. BlipNode initiated link establishment makes it possible use the BlipNode for:

- BlipNet Mobility
- BlipNode initiated PAN sessions
- Establish Serial Port Connections (SPP) to SPP Servers.
- Push of Obex Objects and pull of Business Cards to/from OPP Servers.
- Perform Obex File Transfer with remote Obex FTP Servers.

BlipNode initiated link establishment can only be performed from the BlipNet API or as part of the BlipNet Mobility Solution.
BlipNodes with this configuration cannot be found from other devices by doing inquiry, nor is it possible for other Bluetooth devices to establish a connection to the BlipNode.

Tracking Node

This pre-defined configuration has been made to help application developers implement tracking applications where inquiry results are needed from many BlipNodes. Normally the application developer will need to get a handle and a lock on each BlipNode to start the inquiry. This can be avoided by using this configuration.

This configuration should only be used for the scenario described above.

BlipNodes with this configuration cannot be found from other devices by doing inquiry, nor is it possible for other Bluetooth devices to establish a connection to the BlipNode.

Server Node

This pre-defined BlipNode configuration includes all BlipNet Bluetooth Services, i.e. LAN Access, PAN NAP, FTP and OPP server. This means that all these services are available simultaneously on BlipNodes with this configuration. Seven devices can be connected to the BlipNode simultaneously.

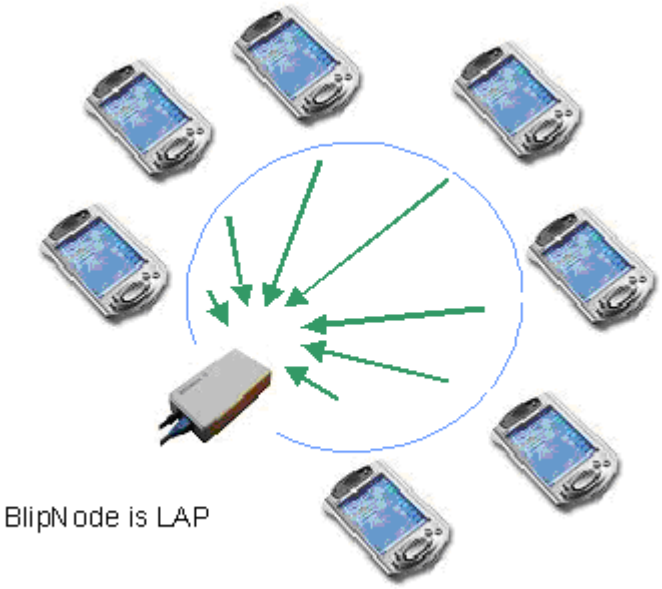
BlipNodes with this configuration can be used for both outgoing and incoming connections.

BlipNodes with this configuration can be used for the BlipNet mobility solution.

The services are described shortly in the following.

LAN Access

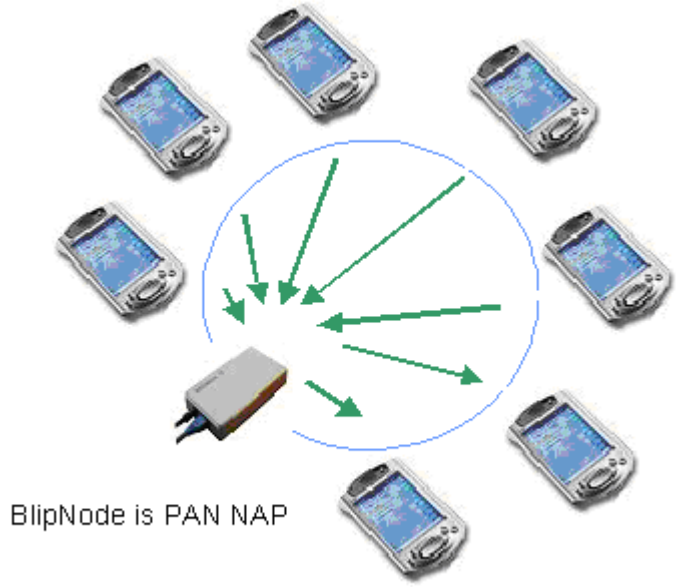
The LAP profile defines how Bluetooth enabled devices can access the services of a LAN using PPP (Point to Point Protocol). LAN access is a basic part of BlipNet. LAN access allows the client device to run Internet applications such as e-mail, web-browsing, etc.



PAN NAP

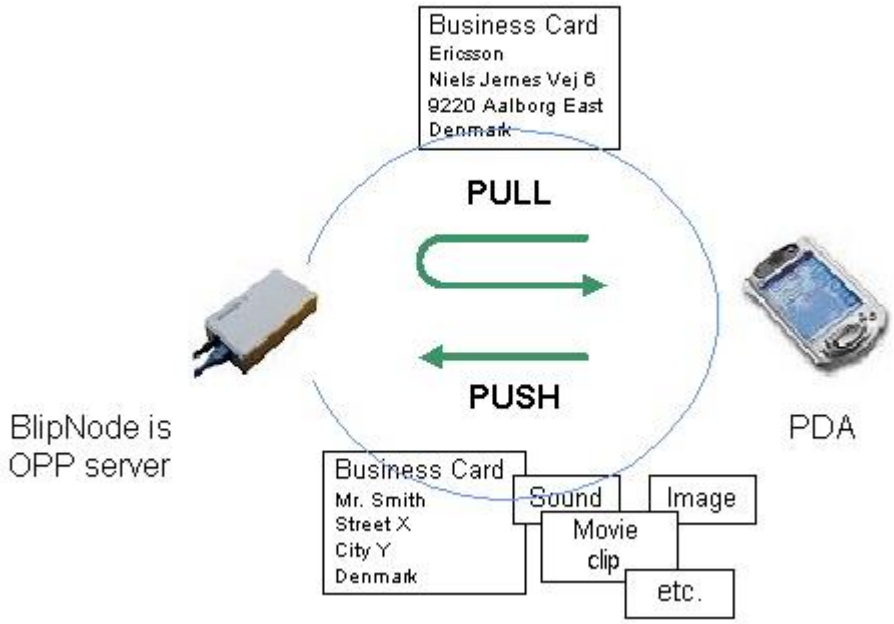
A BlipNode with the PAN NAP service enabled provide the facility for applications to use IP and other networking protocols. NAP is an abbreviation of Network Access Point. A PAN NAP user is called a PANU (PAN User). The behaviour of the a NAP is similar as a network hub. The NAP allows a PANU device to run Internet applications such as e-mail, web-browsing, etc.

When the PAN NAP service is enabled in a BlipNode it can be used for BlipNet Mobility and it is also possible to make NAP initiated PAN session establishment. A BlipNet application must be implemented to do this.



OPP Server

The Object Push Profile (OPP) server configuration facilitates the exchange of business cards and reception of objects such as images, messages, etc.



The BlipServer stores all retrieved objects in the OPP storage root folder and applications can subscribe to notification events from the BlipNet API when new objects are received.

A BlipNode can be used as an OPP server and it is able to receive objects without writing any specific application. Received objects, such as business cards will, by default, be placed in the

folder /opt/blipnet/Obex/OPP. However, this folder can be changed, see the BlipServer Properties - Advanced section.

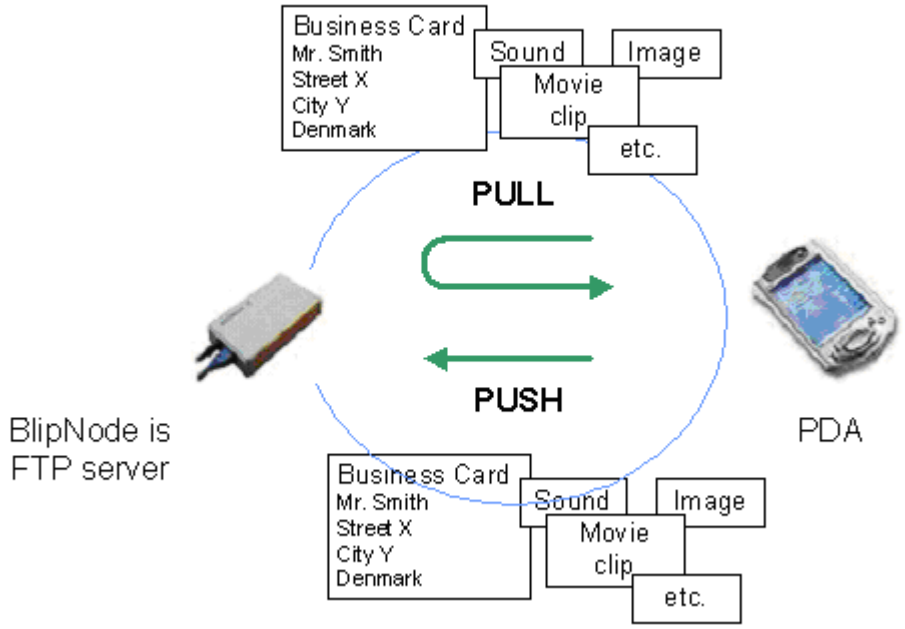
If the OPP server should answer with your business card (instead of the BlipNet Business card) when requested from OPP clients, follow the steps described below:

1. Create a business card, e.g. by using Microsoft Outlook. The official site of vCard is www.imc.org/pdi/, where the format is described.
2. Replace the default Business card located in <blipnet install folder>\properties\default.vcf with the one created in step 1.

Devices doing Business Card Exchange or Business Card Pull will now receive your Business Card.

FTP Server

The File Transfer Profile (FTP) Server give users access to a Bluetooth Obex Based FTP Server. With a dedicated Obex FTP Client on a remote terminal, users will be able to read, write, create and delete files and folders in a root folder specified in the BlipServer.



A BlipNode can be used as a FTP Server without writing any specific application. The File structure will, by default, be placed in the folder <blipnet install folder>/Obex/FTP. However, this folder can be changed, see the BlipServer Properties - Advanced section.

Unconfigured

When a new BlipNode is connected to the LAN and the BlipNode has not previously been configured, the BlipNode will automatically be assigned the empty configuration called “Unconfigured”. A BlipNode having the “Unconfigured” configuration is not active.

Making a new BlipNode Configuration

A new configuration can be created in two ways, either by creating a new configuration from the default template or by duplicating an existing configuration.

- "New" button
  In this case a new clean configuration is made.

- "Duplicate" button
  By clicking on one of the standard configurations and then clicking on the "Duplicate" button a new configuration is created based on the same settings as the standard configuration.

Whichever method used, a configuration wizard will pop up. This wizard will guide you through the creation of the new configuration. The wizard has four steps:

- Configuration name:
  Define the name of the configuration group.

- BlipNode Accessibility:
  Define settings for remote devices to access a BlipNode.

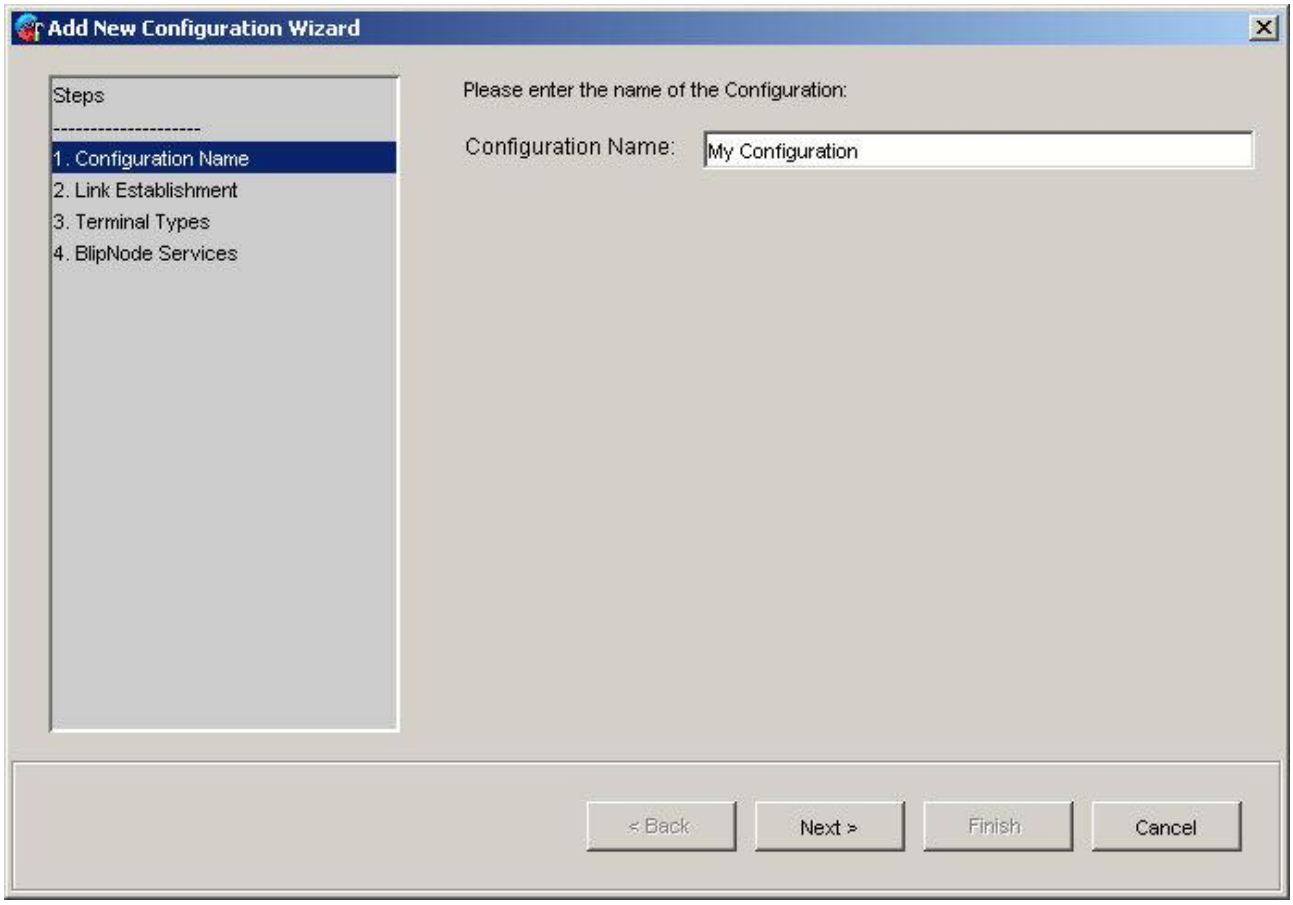
- BlipNode Services:
  Definition and configuration of the BlipNode services.

Configuration Wizard

Configuration Name

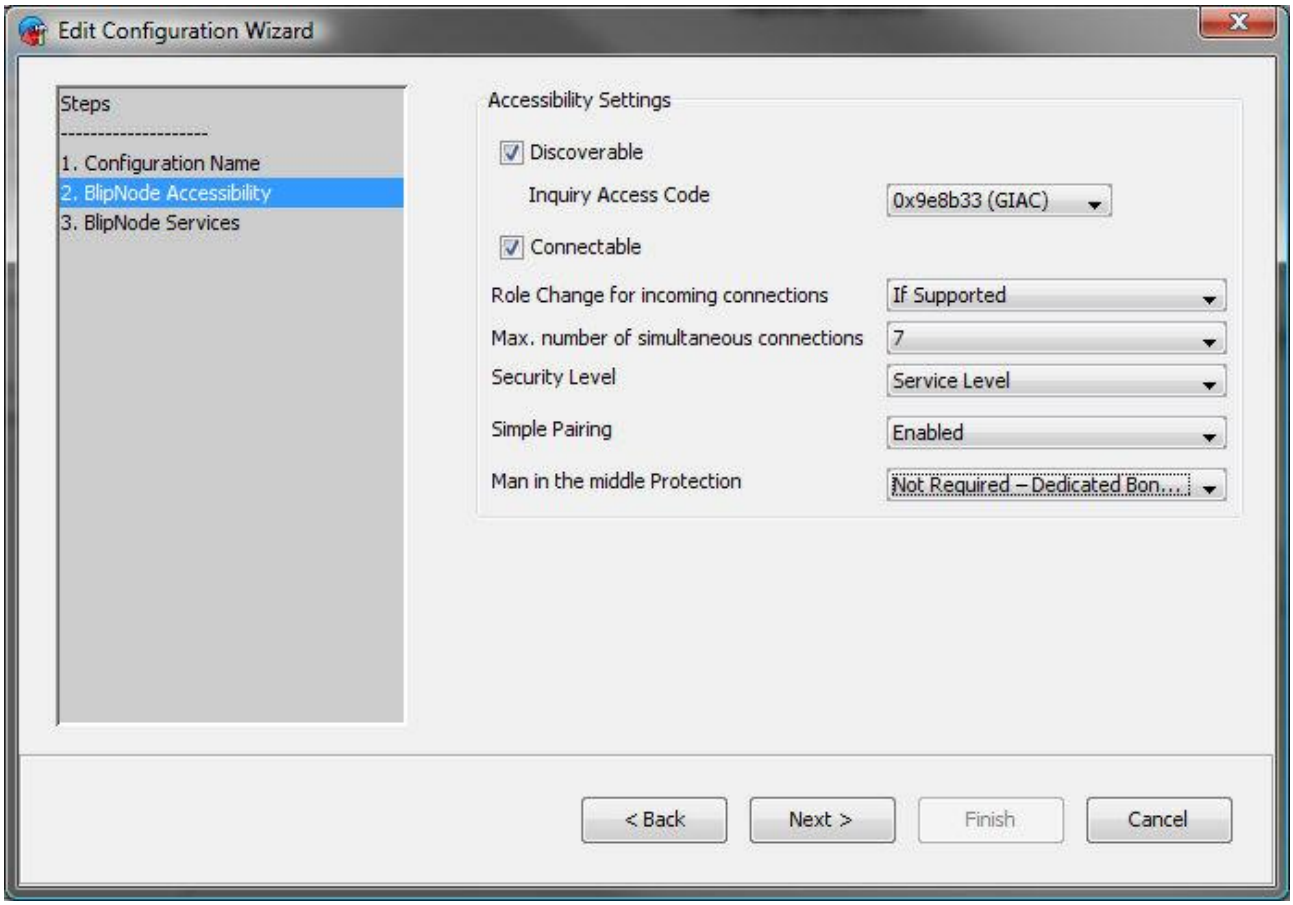
In the first step of the configuration wizard the name of the configuration shall be inserted.

The configuration name must be unique. Two configurations cannot have the same configuration name.



BlipNode Accessibility

The second step in the configuration wizard is the BlipNode Accessibility step. Via this window settings regarding accessing the BlipNode can be configured.



Discoverable
If checked, the BlipNode will be discoverable (other Bluetooth devices can discover the BlipNode).

Inquiry Access Code
Configures the Access Code that the Bluetooth Radio will listen for during inquiry scan. This must always be set to General Inquiry Access Code (GIAC).

Connectable
If checked on, then the BlipNode will be connectable (other Bluetooth devices can establish a connection to the BlipNode).

Role Change
The field can have the values:

- Not required — When this value is used the BlipNode will not force master/slave switch. This setting shall be used when it is known that only one device is connected to the BlipNode at the time.
- Required — When this value is used the BlipNode will require all connecting

devices to perform master/slave switch. If this setting is not used and if the BlipNode acts as access point, only one connection at the time will be supported.

- If supported — This is a special feature, which should normally be avoided, because if a terminal without support for master/slave switch connects to the BlipNode, the BlipNode is blocked for further connections until this device is disconnected.
  With this value selected, the BlipNode will allow devices without support for master/slave switch to connect without performing the switch. If a device supporting master/slave switch connects, a switch is made.

Max. number of simultaneous Connections
A BlipNode can handle from 1 to 7 simultaneous connections.

Security Level
Following levels exist:

- No Security — This implies that the BlipNode will not require any authentication of the client nor will encryption be invoked from the BlipNode.
- Link level — This implies that the BlipNode will require authentication of any connecting device and the BlipNode will enforce encryption. Enabling Link level security implies that the remote device will not be able to even discover the available services on a BlipNode without entering a valid Bluetooth Passkey. This level is normally not used.
- Service Level — This is the level normally used. Service level implies that authentication and encryption can be required at a point in the connection establishment phase where the intention of the connecting terminal is known. This makes it feasible for example to require authentication/encryption for LAN access clients accessing the LAN, but allow all devices to put objects to BlipNet without any authentication. As it will be seen in step 4 of the configuration wizard "BlipNode Service", security can be enabled/disabled per service when the security level is set to "Service Level".

Simple Pairing
Secure Simple Pairing simplifies the pairing procedure for the user.
Secondary it improves the security in Bluetooth wireless technology with protection against passive eavesdropping and protection against man-in-the-middle (MITM) attacks (active eavesdropping).

Secure Simple Pairing requires Bluetooth 2.1 and can only be enabled for the BlipNode L2i product.

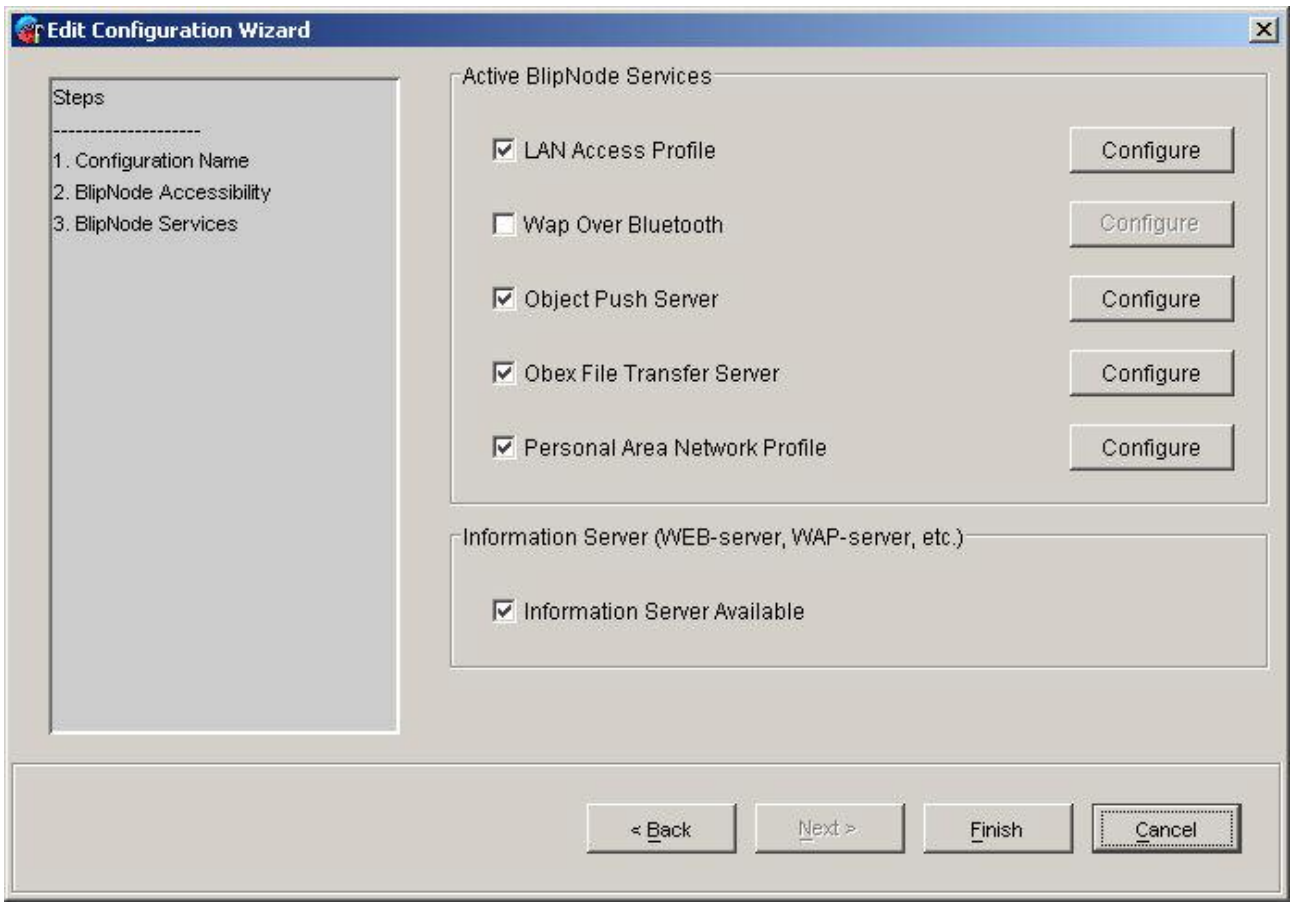
Man in the Middle Protection
Man in the Middle Protection setting for Simple Pairing.

Not Required – No Bonding.	No Bonding. Numeric comparison with automatic accept allowed.
Not Required – Dedicated Bonding.	Dedicated Bonding.Numeric comparison with automatic accept allowed.
Not Required – General	General Bonding. Numeric Comparison with automatic

Bonding.	accept allowed.

BlipNode Services

The 3th step in the "Configuration wizard" is the "BlipNode Services" step. This window is used to configure which services the BlipNode shall advertise towards connecting terminals.



Following services can be activated on a BlipNode:

- LAN Access Profile — This service must be activated if the BlipNode shall enable LAN Access clients, such as PCs, PDAs etc. to access the LAN behind the BlipNode.
- WAP Over Bluetooth — This service must be activated if the BlipNode shall allow WAP clients, such as phones to connect to a WAP gateway on the LAN behind the BlipNode.
- Object Push Server — This service must be activated if the BlipNode shall allow devices with object transfer facilities to push objects such as e.g. business cards to the server.
- Obex File Transfer Server — This service must be activated if the BlipNode shall allow devices with File Transfer facilities to get and put files to the server
- Personal Area Network Profile — This service must be activated if the BlipNode shall enable PAN users (clients) to access the LAN behind the BlipNode.

To configure the settings for a service click on the corresponding "Configure" button.

Information Server
This checkbox is only changeable if the LAN access profile is checked. It must be checked if some kind of WEB or WAP server is available on the LAN connected to the BlipNode.

BlipNode Services

LAN Access Profile Settings

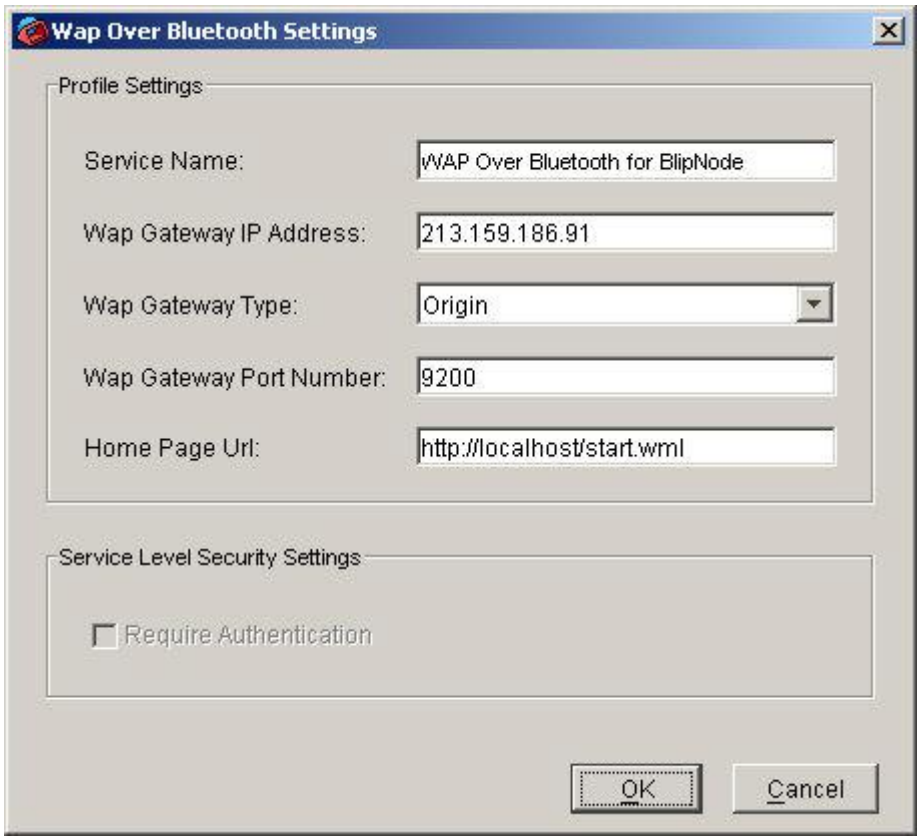
Service Name
This is a free text string, which will be shown as the name of the service on the GUI on a connecting device. The Service Name parameter is a short user-friendly name for the service; for example "Corporate Network", "Conference#1", etc.

Service Description
This is a free text string, which might be shown on the GUI on a connection device. The Service Description attribute is a longer description of the service. For example "This network is provided for our guests. It provides free Internet Access and printing services. No user name or password are required."

Require Authentication
This checkbox must be checked if authentication of connecting devices must be performed. If this checkbox is checked also encryption of traffic will be made. If the security level (specified in the BlipNode Accessibility window) is "Link Level" or "No Security", the checkbox is grayed out and can then not be enabled or disabled.

WAP Over Bluetooth Settings

The WAP over Bluetooth service can be used when the BlipNet is used with special "WAP Over Bluetooth" enabled terminals. Bluetooth Networks has developed WAP over Bluetooth software for several Sony-Ericsson terminals. With this software it is possible to run a WAP session over Bluetooth. By writing an application it is even possible to make WAP push functionality over Bluetooth.



Service Name
This is a free text string, which will be shown as the name of the service on the GUI on a connecting device.

WAP Gateway IP Address
The IP address of the WAP gateway. By providing this address no configuration of the connecting WAP Client device is required.

WAP Gateway Type
The gateway type can either be "Origin" or "Proxy". If the type is set to origin a connecting WAP client can store WAP bookmarks together with specific Bluetooth device address of the BlipNode. The "Origin" option shall only be used when just one BlipNode is configured for WAP over Bluetooth, otherwise the "Proxy" setting shall be used.

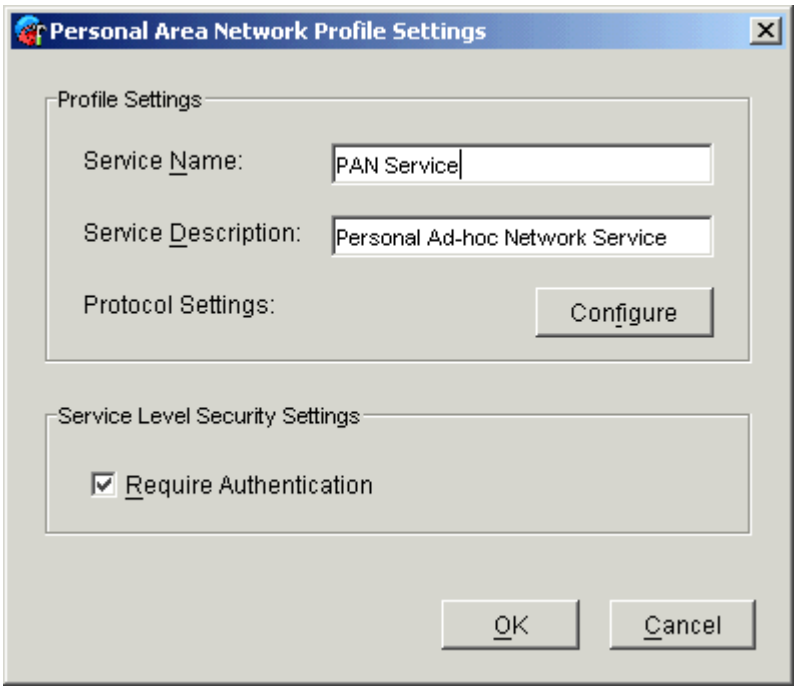
WAP Gateway Port Number
The port number, which the WAP client must connect to on the WAP gateway.

Home Page Url

The home page of the WAP service available via the BlipNode.

Require Authentication
Cannot be changed, the authentication settings for LAN Access is used for WAP Over Bluetooth.

Personal Area Network Profile Settings



Service Name
This is a free text string, which will be shown as the name of the service on the GUI on a connecting device. The Service Name parameter is a short user-friendly name for the service; for example "Corporate Network", "Conference#1", etc.

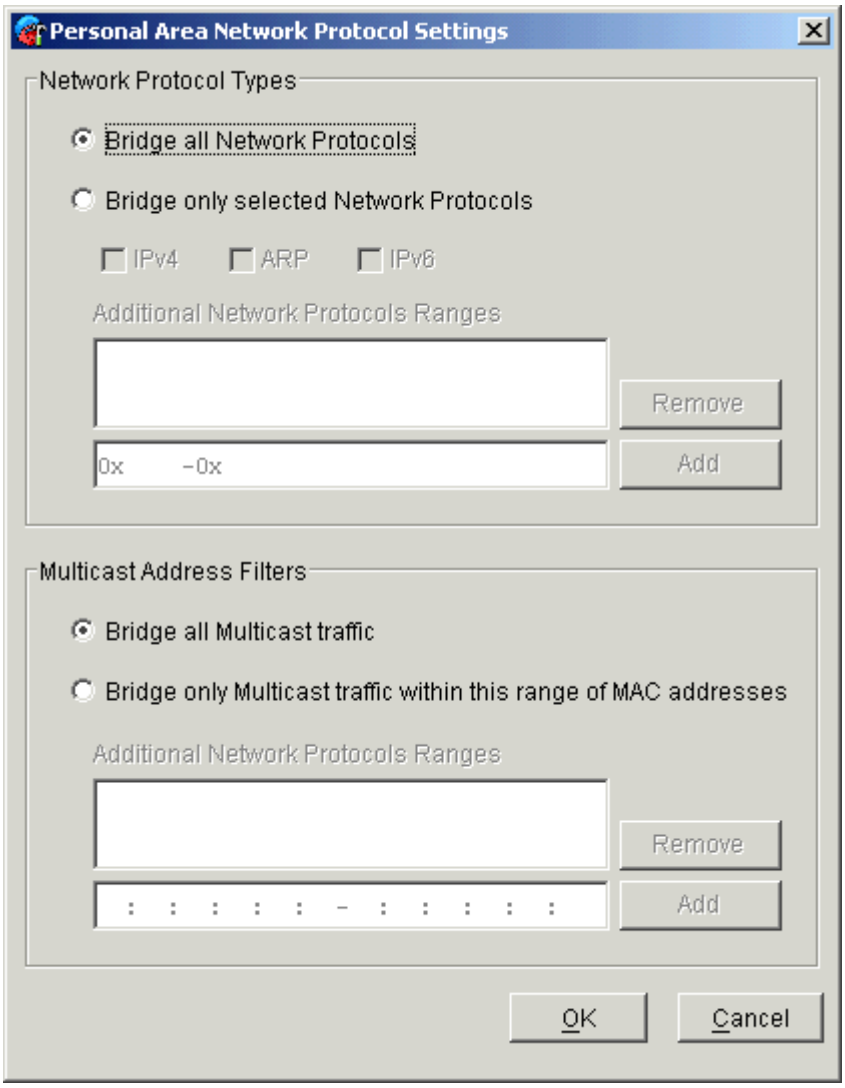
Service Description
This is a free text string, which might be shown on the GUI on a connection device. The Service Description attribute is a longer description of the service. For example "This network is provided for our guests. It provides free Internet Access and printing services. No user name or password are required."

Protocol Settings
PAN protocol settings can be configured in a Personal Area Network Protocol Settings window when pressing the configure button.

Require Authentication
This checkbox must be checked if authentication of connecting devices must be performed. If this checkbox is checked also encryption of traffic will be made. If the security level (specified in the BlipNode Accessibility window) is "Link Level" or "No Security", the checkbox is grayed out and can then not be enabled or disabled.

Personal Area Network Protocol Settings

In the PAN profile two types of filtering can be made. They are Network Protocol Type filtering and Multicast Address filtering. Network Protocol Type filtering is filtering of Ethernet frames dependent on the Network Protocol Type. Multicast Address filtering is filtering of multicast Ethernet frames dependent on their destination multicast address.



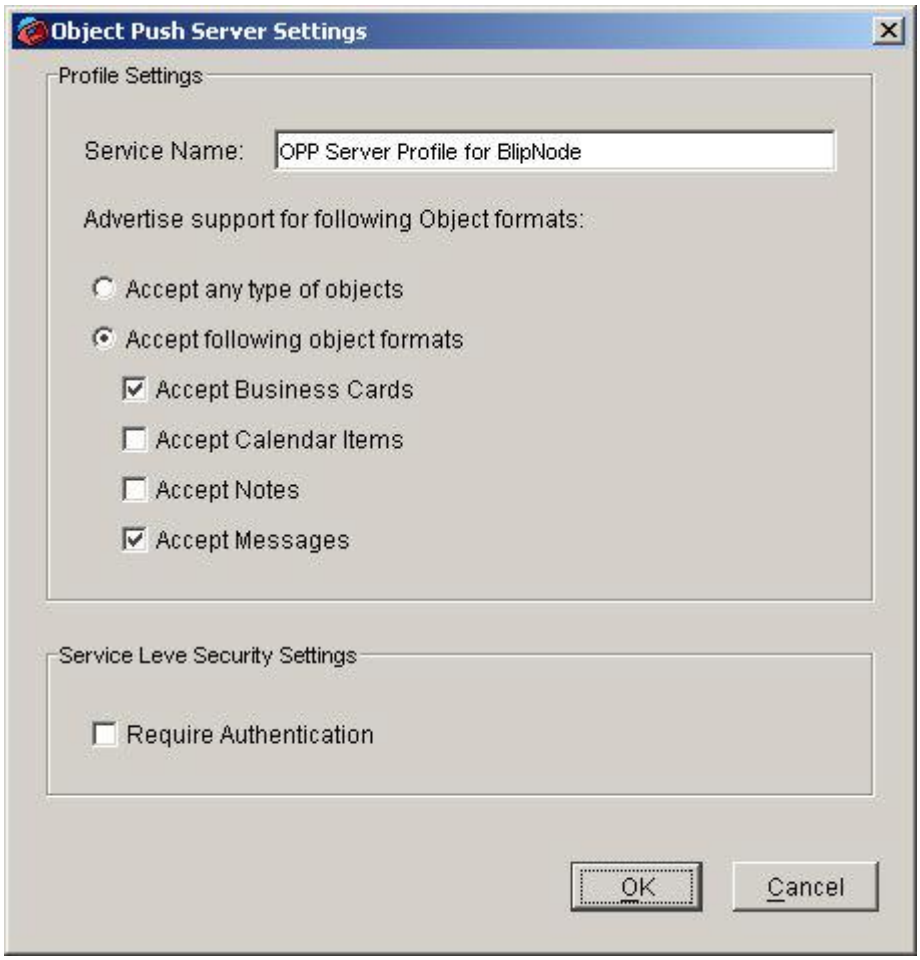
In the Personal Area Network Protocol Settings window it possible to specify a filter on Network Protocol Types and on Mutlicast Addresses. The specified filters will be set both locally in the BlipNode and remotely on connected PAN devices. The specified filters are set on a remote device as soon as it establishes a PAN session to the BlipNode.

The default PAN filter settings in a BlipNode Configuration including PAN are no filtering at all, this means that the BlipNode bridges all network protocol types and bridges all multicast traffic to connected PAN devices.

Network Protocol Type numbers can be found on: http://www.iana.org/assignments/ethernet-numbers

In most network scenarios it is not necessary to configure a BlipNode with PAN filters. If filtering is wanted by a connected PAN device, it can configure the BlipNode remotely with specific PAN filters.

Object Push Server Settings



Service Name
This is a free text string, which may be shown as the name of the service on the GUI on a connecting device.

Supporting object formats
It can either be chosen to accept any type of objects or to only accept specified object formats. When only specific object formats must be accepted, following object formats can be chosen:

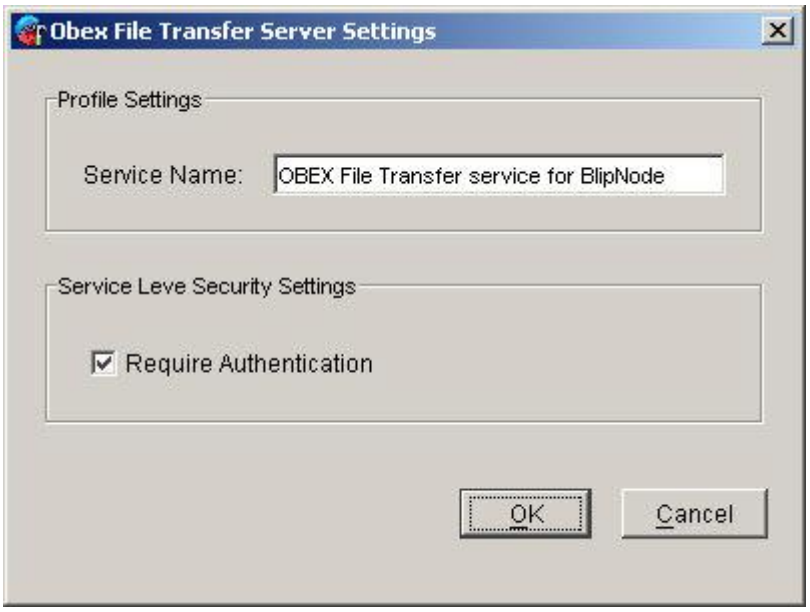
- Business Cards — This includes both vCard 2.1and vCard 3.0 formats.
- Calendar Items — This includes both vCalendar 1.0 and iCalendar 2.0 formats.
- Notes — This includes the vNote format.
- Messages — This includes the vMessage format.

For more information about the specific object formats, see The Internet Mail Consortium http://www.imc.org/.

Require Authentication

This checkbox must be checked if authentication of connecting devices must be performed. If this checkbox is checked also encryption of traffic will be made. If the security level (specified in the BlipNode Accessibility window) is "Link Level" or "No Security", the checkbox is grayed out and can then not be enabled or disabled.

File Transfer Server Settings



Service Name
This is a free text string, which may be shown as the name of the service on the GUI on a connecting device.

Require Authentication
This checkbox must be checked if authentication of connecting devices must be performed. If this checkbox is checked also encryption of traffic will be made. If the security level (specified in the BlipNode Accessibility window) is "Link Level" or "No Security", the checkbox is grayed out and can then not be enabled or disabled.

BlipNet Mobility

BlipNet Mobility Service

The BlipNet mobility service enables seamless wireless network connectivity for Bluetooth enabled devices. The mobility service automatically connects to subscribed devices when they enter BlipNet coverage, and automatically hands over terminals from zone to zone as they move around.

The BlipNet mobility service is based on the Bluetooth PAN profile which is basically a wireless Ethernet bridge.

Mobility Zones

A mobility zone is a group of one or more BlipNodes defined in the BlipManager mobility settings. All BlipNodes in a zone should be deployed in the same physical location. BlipNodes in a zone can be defined as Discovery and Access Nodes, or Access only nodes.

Discovery Nodes

One BlipNode in each zone must be configured to periodically search for terminals. Due to the fact that inquiry has a negative impact on data transfer rates, there is a trade-off between discovering terminals quickly and ensuring a high data rate for connected devices. The interval with which the BlipNode searches for terminals is configurable in the BlipManager mobility settings; however, the default setting of 20 second intervals is recommended for most cases.

Adding Access Nodes to High Density Zones

If there is a high penetration of devices in a zone, or if there are high bandwidth requirements for each device, more access nodes can be added to a zone. If multiple nodes are added to a zone, the BlipNet Mobility Service does automatic load balancing between these nodes.

Supported Devices

Devices subscribed to the mobility service must support the Bluetooth PAN profile, and for the hand-over functionality, Bluetooth scatternet support is required in the device. Examples of devices supporting both PAN and scatternet is the HP iPAQ h1940, h2210 or similar, as well as many Bluetooth PC dongles.

Older devices

Devices which do not support scatternet (such as older iPAQs and PC cards) can be automatically connected by the system; however, when moving from zone to zone, the connection will be disconnected briefly.

Pre-configuring BlipNodes

The BlipNodes which are to be used in the BlipNet Mobility Service must be pre-configured via the BlipManager. A number of configuration options affect the Mobility Service:

PAN Service: The PAN service **must** be enabled in all BlipNodes in the Mobility Service.

Discoverable and Connectable Modes: If you are using only devices supported by the Mobility Service, the BlipNodes can be set non-discoverable and non-connectable for added security. This will ensure that other devices cannot detect and connect to the BlipNodes.

Master/Slave switching: If the BlipNodes are discoverable and connectable, master/slave switching should be set to *Required*. Otherwise, an incoming connection could block the BlipNode for use by other devices.

Standard configurations

For a pure mobility system, putting the BlipNodes in the "*Client Node (No Services)*" configuration is the optimal and most secure solution. BlipNodes in this configuration are not discoverable or connectable, and the PAN service record is the only active service.

If you want to allow users to make incoming PAN connections or need to connect devices which only support the older LAN Access Profile, the BlipNodes must be configured with the LAN Access service record, and the BlipNodes must be both discoverable and connectable. For this purpose, the "*Server Node (All Services)*" configuration is a suitable choice.

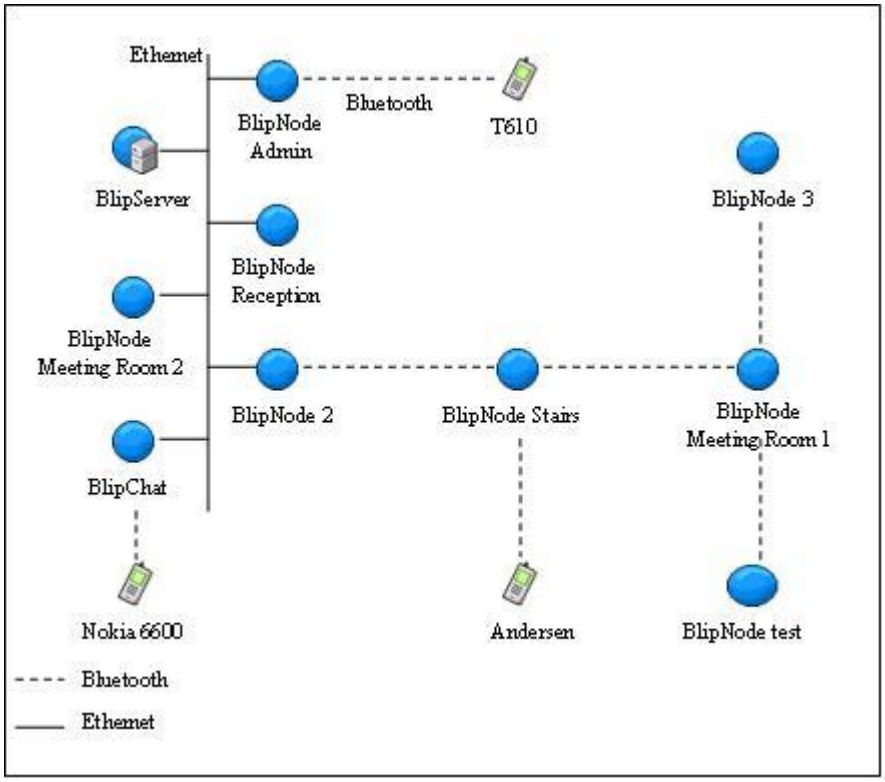
Note! Users of LAN Access devices need to connect manually to the nearest access point, and the devices should not be registered as mobility terminals, because the mobility service will fail to connect to them.

Wireless BlipNodes

About Wireless BlipNodes

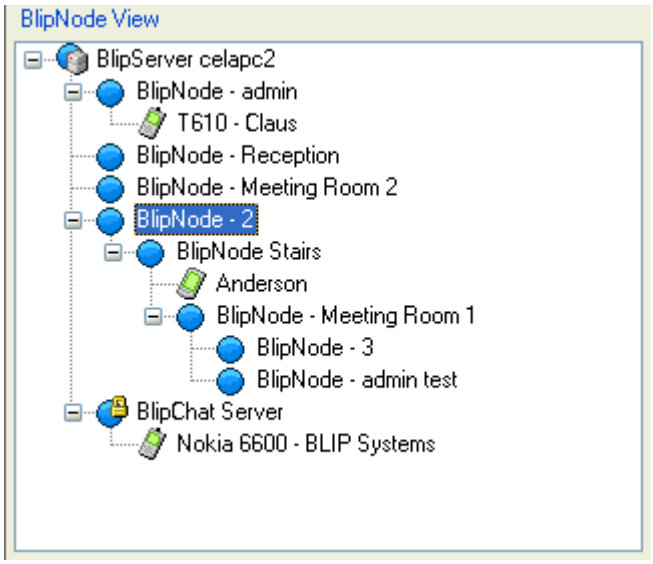
BlipNet allows BlipNodes to be connected to the BlipServer through other BlipNodes instead of Ethernet.

Below is shown a setup with wireless BlipNodes.



The BlipServer will instruct 'BlipNode - 2' to establish a Bluetooth PAN connection to 'BlipNode - Stairs'. When 'BlipNode Stairs' has allocated an IP Address and registered itself on the BlipServer, the BlipServer will instruct 'BlipNode - Stairs' to establish a Bluetooth PAN connection to 'BlipNode - Meeting Room 1' and so on.

In the BlipManager, the BlipNode tree View will show the Wireless Topology like the figure below.



There are some important things to notice about Wireless BlipNodes

1. Wireless BlipNodes must not be connected to the ethernet.
2. A Wireless BlipNode offers the same functionality as a Ethernet BlipNode but have a maximum of 6 active connections as one is used for the Backbone connection.
3. The Bluetooth bandwidth for wireless BlipNodes are limited compared to BlipNodes connected through Ethernet. Use wireless BlipNodes with care.

For information about configuring Wireless BlipNodes, please read the section BlipNode View

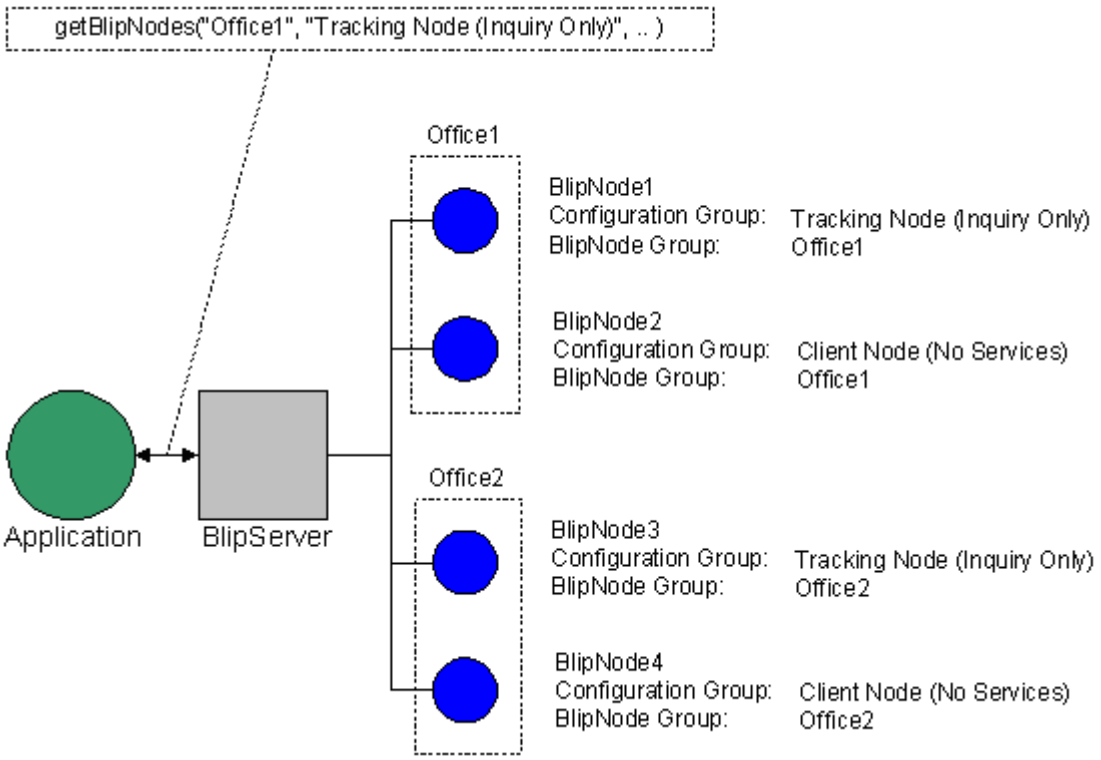
Howto

Using the BlipNode Groups Concept

The BlipNode Group is a logical term which has been introduced to be able to distinguish groups of BlipNodes from each other in an application without knowing the Bluetooth address of the BlipNode. Using this concept, an application becomes independent of e.g. hardware replacements.

From the BlipManager it is possible to create a BlipNode Group and to assign BlipNodes to this group. It is then possible for an application to find a BlipNode belonging to a group without knowing the Bluetooth device address of the BlipNode.

A BlipNode Group is not the same as a Configuration Group. BlipNodes in the same Configuration Group share the same basic configuration. BlipNodes in the same BlipNode Group do not necessarily have the same basic configuration. A BlipNode Group consists of a number of BlipNodes used in a specific use case or application.



The figure above illustrates an example of the BlipNode Group concept where BlipNodes are placed in two different BlipNode Groups, "Office1" and "Office2". Go to section BlipServer Properties - BlipNode Groups to see a description of how to create a BlipNode Group.

Configuration of BlipNet for BlipNet API applications

When writing an application on top of the BlipNet API, certain configurations must be made in the BlipManager. The following is a short checklist:

1. Create a “User account” for the application. Creating a “user account” includes defining a login and a password, which can be used by the application when connecting to the BlipNet API. Go to the BlipServer Properties - User Accounts section to see a description of how to create a “User Account”.
2. Configure the BlipNode to be used by the application. The available standard configurations are described in section General about BlipNode Configurations. Custom configurations can also be made, see section Making a new BlipNode Configuration.
3. It is recommend to write applications that are independent of the Bluetooth address of the BlipNode, see section Using the BlipNode Groups Concept.

Diagnostics

Diagnostics

When connecting terminals, problems might occur due to:

- Wrongly configured DHCP servers
- Wrongly configured terminals
- Wrongly configured BlipServer

The most common problems are:

- BlipNode does not connect to the BlipServer
- Problem when connecting to LAN access service in BlipNet
- Problem when connecting to the OPP server in BlipNet
- Problem when pushing objects to the OPP server in BlipNet
- Problem when pushing from BlipNet to an OPP server device

BlipNode does not connect to the BlipServer

If a BlipNode is attached to the LAN where the BlipServer is running and the BlipNode is not found by the BlipNet within approx. 30-60 seconds, something is wrong. Every time the BlipNode is switched on, it will search for a BlipServer. This search will be repeated every 30 seconds.

By looking at the BlipManager Main window, it can be verified whether the BlipNode is connected to the BlipServer or not. A connected BlipNode is displayed with black text and a blue BlipNode icon. A disconnected BlipNode is displayed with grey text and a grey BlipNode icon.

If the BlipNode does not find the BlipServer, please try the following procedure to locate the problem:

1. Check that you have valid license file installed and enough BlipNode licenses. Please refer to Getting Started and BlipServer Properties->General Panel

2. Check if the BlipNode has retrieved an IP address.
   Try to ping the network broadcast address. The network broadcast address depends on the specific network configuration.

   An example of a broadcast address:
   The subnet mask is 255.255.255.0
   The network address is 101.102.103.00
   On this network the network broadcast address is 101.102.103.255.

   Try to ping all BlipNodes on this subnet via a command prompt and then check the arp table of the BlipServer.

   In Windows ping by typing:
   ping 101.102.103.255

   In Linux ping by typing:
   ping –b 101.102.103.255

   Check the arp table by typing following in a command prompt:
   arp –a

   Next try to find the "MAC" address of the BlipNode in the arp table to see if an IP address has been assigned. The MAC address of the BlipNode can be seen on the white label on the BlipNode.

3. If the BlipNode is found in the arp table, the BlipNode has an IP address. Go to step 3. If the BlipNode does not have an IP address, go to step 4.

4. The BlipNode has an IP address. If the BlipNode does not connect to the BlipServer this can be due to any one of 4 reasons:

   a. The BlipServer does not allow all BlipNodes to connect and the specific BlipNode is not listed as one of the allowed BlipNodes.
      Solution: Add the BlipNode to the "BlipServer Allowed BlipNodes List", or allow all BlipNodes to connect to the BlipServer.

b. There is more than one BlipServer on the net and another BlipServer has "stolen" the BlipNode.
Solution: Use the white list in all BlipServers on the LAN to specify which BlipServer the BlipNode belongs to.

c. The BlipNode has outdated software which is not compliant with the current BlipServer.
The software package distributed with BlipNet 1.0 is able to upgrade BlipNet 0.5 BlipNodes. If the BlipNode is older than this, it must be upgraded to 0.5 first.
Solution: Upgrade the BlipNode to the 0.5 software and start the auto update BlipNode software, see the BlipServer Properties - Advanced section.

d. Software upgrade of a BlipNode has failed and the BlipNode is in FTP server mode. Looking at the yellow LEDs on the BlipNode can verify this. If the blink sequence is SOS in Morse * * */ - - -/ * * * (3 short, 3 long, 3 short flashes) the BlipNode is in FTP server mode.
Solution: Please make sure that automatic software upgrade is switched on (see the BlipServer Properties - Advanced section) and try to restart the BlipNode.

5. The BlipNode did not retrieve an IP address. Several possible reasons exist. Please check the following:

a. Make sure that a DHCP server is present on the network. If there is no DHCP server, please refer to the "Configuration" section in the BlipNet installation guide to start a DHCP server.

b. Make sure that the DHCP server has not run out of IP addresses. There is a fixed limit on the number of available addresses. Both terminals (LAN access clients only) and BlipNodes receive an IP address from the DHCP server, so if many LAN access clients are connected, this might cause a BlipNode not to be able to connect to the BlipServer, because the IP address limit has been reached. To check if this is the case try to disconnect all other terminals / BlipNodes and see if this solves the problem. If so, re-configure the DHCP server to have more IP addresses.

c. The BlipNode did not start up properly, e.g. after a software upgrade. Please refer to the BlipServer Properties - Advanced section.

d. The BlipNode might have received an IP address, but it is not in the arp table. It may not have received the ping because it is on another subnet. Please make sure that the BlipNode is placed on the same subnet as the BlipServer. The BlipNode and the BlipServer find each other via UDP broadcast.

Problem when connecting to LAN access service in BlipNet

Before going through this procedure please make sure that the correct configuration is used. Either the "LAN Access", the "LAN Access and Object Push Server" configuration or another suitable custom configuration must be used. If the problem remains then the procedure to find the problem depends on what the problem appears to be from the terminal side.

From the terminal side the following might happen:

1. The terminal cannot find the BlipNode in a device discovery.
2. The terminal cannot make a service search on the BlipNode.
3. The LAN access service is not available after making a service search.
4. The terminal cannot make a PPP connection.

The solutions to the different problems are listed below:

1. If the terminal cannot find the BlipNode in a device discovery, it can be due to the following reasons:

    a. First make sure that the BlipNode you are trying to connect to is attached to the BlipServer. It must be shown with black text and a blue BlipNode icon in the BlipManager configuration view tree.

    b. Then make sure that the BlipNode is in discoverability mode. This will be the case if a proper standard configuration has been used. If a custom configuration is used, see section Link Establishment - Customize.

2. The terminal cannot make a service search on the BlipNode.Please check that the Terminal is not set to "Never" in BlipServer Properties -> Terminals or to "Default" if "Allow all Terminals to Connect" is de-selected. Also check the specific BlipNode is not configured with a "BlipNode Disallowed Terminal List", this might cause the problem. Please see section BlipNode Properties - Allowed Terminals and section BlipServer Properties - Terminals. for future details.

3. The LAN access service is not available after making a service search.
   Please make sure that the LAP access record is enabled, see section BlipNode Services.

4. The terminal cannot make a PPP connection. On some terminals a PPP connection is automatically established after establishment of a LAN access session. The BlipNode will try to retrieve an IP address to the terminal when the terminal tries to connect to the LAN access service. If the DHCP allocation fails, the terminal will not be able to make a successful LAN access connection. The DHCP allocation might fail due to the following reasons:

    a. Check if the DHCP allocation has failed due to a lack of IP addresses. Please see section BlipNode does not connect to the BlipServer, item 4.b.

    b. Please check whether the DHCP server supports broadcast or unicast to the DHCP clients. For more information see the issues of DHCP configurations in section BlipServer Properties - Advanced.

Problem when connecting to the OPP server in BlipNet

Before going through this procedure please make sure that the correct configuration is used. Either the "Object Push Server", the "LAN Access and Object Push Server" configuration or another suitable custom configuration must be used.

If the problem remains then the procedure to find the problem depends on what the problem appears to be from the terminal side. The following problems and solutions are known:

1. If the terminal cannot find the BlipNode in a device discovery, it may be due to the reasons listed in section BlipNode Does Not Connect to the BlipServer item 1.

2. The terminal cannot make a service search on the BlipNode. This may be due to several reasons, see section BlipNode Does Not Connect to the BlipServer item 2.

3. The OPP service is not available after making a service search. Verify that the Object Push Server service is enabled, see section BlipNode Services.

Problem when pushing objects to the OPP server in BlipNet

If pushing objects to the OPP server in BlipNet fails, there are some possible problems and solutions. The following problems and solutions are known:

1. A lack of disk capacity on the BlipServer. Check the disk capacity on the machine on which the BlipServer is running. There must be enough disk capacity for incoming objects.

2. The object format of the object being pushed is not supported. See section Object Push Server Settings describing how to verify that the object format is supported.

3. Bad radio link. The reason for a failure when pushing an object to BlipNet may also be a bad radio link if the terminal moves out of range. Please move the terminal back into range and try again.

Problem when pushing from BlipNet to an OPP server device

If pushing from a BlipNet to a terminal having the OPP service fails, several possible reasons exist. Problems might occur at different levels in the push phase. Before going through this procedure please make sure that the correct configuration is used. Either the "Object Push Client", the "T68i WAP Terminals" or another suitable custom configuration must be used.

If the problem remains then the procedure to find the problem depends on where in the process it fails. The following problems and solutions are known:

1. If the BlipNode never finds any devices. Please make sure that the devices to be pushed to are discoverable. This can normally be configured in the menus on the device itself.

2. If the BlipNode does not connect to the device. This may be due to several reasons:

    a. The device is in the "BlipServer Disallowed Terminal List" or in the "BlipNode Disallowed Terminal List" for the specific BlipNode. Please make sure that this is not the problem. Please see section BlipServer Properties -Allowed Terminals and section BlipNode Properties - Allowed Terminals.

    b. The device did not have the services required. If the remote device did not have the OPP server, it is simply impossible to push to the device.
    Verify that Terminal Types / Services for allowed terminals are configured correctly, see the Terminal Filtering Wizard section Terminal Types and section Terminal Services.
    If a device did not have the "Required Services", the BlipNode will put the device in a local disallowed list (this cannot be seen anywhere in the BlipManager). Restarting the BlipNode can only clear this local disallowed list. This functionality has been implemented to prevent an endless loop of failed SDP searches.

Terminology

Terminology

BlipNode Group — A BlipNode Group is a logical name for a collection of BlipNodes. The BlipNodes in a BlipNode Group may have different configurations. A BlipNode Group name may, for example, be a location (e.g. "Reception") or an application name (e.g. "Laptop Detector"). An application developer can use the BlipNode Group name to retrieve the BlipNodes assigned to this particular group from an application.

BlipNode Configuration — A BlipNode Configuration is a set of BlipNodes sharing the same basic configuration. The BlipNodes do not share the exact same configuration - e.g. the friendly name and BlipNode Group may be different.

Friendly name — Every Bluetooth device has a "human" readable name, a string that can be defined as anything, e.g. "Mr. Smith's Ericsson T68i Phone".

Inquiry — A Bluetooth device making an inquiry is searching for discoverable Bluetooth devices within range. When a device is discovered during the inquiry, an application can use this information to set up a connection to the discovered devices (by means of the paging procedure).

Master — In a Bluetooth connection between two devices, one device is the master and the other device is the slave. A Bluetooth device establishing a connection (paging) to another Bluetooth device is said to be the master device in a Bluetooth link. The device accepting the paging is said to be the slave. A device acting as a master is normally able to simultaneously act as a slave for a short period of time before it requires a master / slave switch. Normally a master can have up to 7 simultaneous active connections.

Master / slave switch — When a Bluetooth device (master) connects to another Bluetooth device (slave), the slave might wish to change roles if it already acts as a master for other Bluetooth devices. It is not desirable for a Bluetooth Access Point to be a slave, for example, because then only one Bluetooth device can connect to the access point at a time. Therefore an access point will initially act as a slave, and then as the connection is established, it will require shifting roles such that the access point becomes a master.

Page — When a device wants to connect to a specific known device, it will have to page it to establish a link with it.

Role change — Role change or switching is the same as master/slave switching. See master/slave switch for a description.

Scan — A device listening for either a paging device or a device making an inquiry is said to be scanning.

Slave — See description of slave under master. A slave can normally only

	communicate with one master at a time. A slave can normally only be connected to one Bluetooth device (a master) at a time.
User Account	A set of credentials consisting of a login and a password. Two types of accounts exist, an administrator account and an application account. An application using the BlipNet API must register in the API with a user account.

Index

A
Allowed BlipNodes 35
B
BlipNode Properties 22
Bluetooth bondings.....36
Bluetooth Passkey 36
Bonding 36
Bonds 36
C
Configuration Groups 26
E
Expire Bluetooth.....36
F
Firm Ware 22
FTP Server Version 22
FW Version 22
H
HW Version.....22
P
Pairing 36
PIN 36
R
Require Authentication 36
S
Security 36
Security Settings 36
Service level 36
SW 22
SW Version 22
U
Use
Security Settings..... 36
V
Version Info 22
Version Info window 22